بنك الكويت المركزي
CENTRAL BANK OF KUWAIT

Cyber and Operational Resilience Framework for All Local Banks and Financial Institutions

Table of Contents

Introduction

In an era defined by rapid technological advancement, increased digital interconnectedness, and an ever-evolving sophisticated threat landscape, the resilience of the banking sector has become a national imperative. As the Central Bank of Kuwait, we recognize that our mandate to preserve monetary and financial stability must now be matched by an equally robust commitment to cyber resilience. A resilient banking system fosters a sustainable economic growth, enables digital leadership, public trust, and strengthens Kuwait's competitiveness on the global stage.

The Cyber and Operational Resilience Framework represents the next step evolution in the Central Bank of Kuwait's regulatory strategy, moving from establishing foundational cybersecurity compliance under the Cybersecurity Framework (2020) to a "Resilience-first" and "Maturity-oriented" Regulatory model (2025). It reflects our resolve and determination to empower Regulated Entities not only to defend against cyber threats, but to anticipate, withstand, recover from, and adapt to disruptions with agility and confidence, reinforcing the resilience of the broader banking sector and financial ecosystem of the State of Kuwait.

The aim is to shape a resilient digital future. One that enables innovation, protects national interest, and secures Kuwait's strategic edge in the international financial landscape.

Central Bank of Kuwait

بنك الكويت المركزي
CENTRAL BANK OF KUWAIT

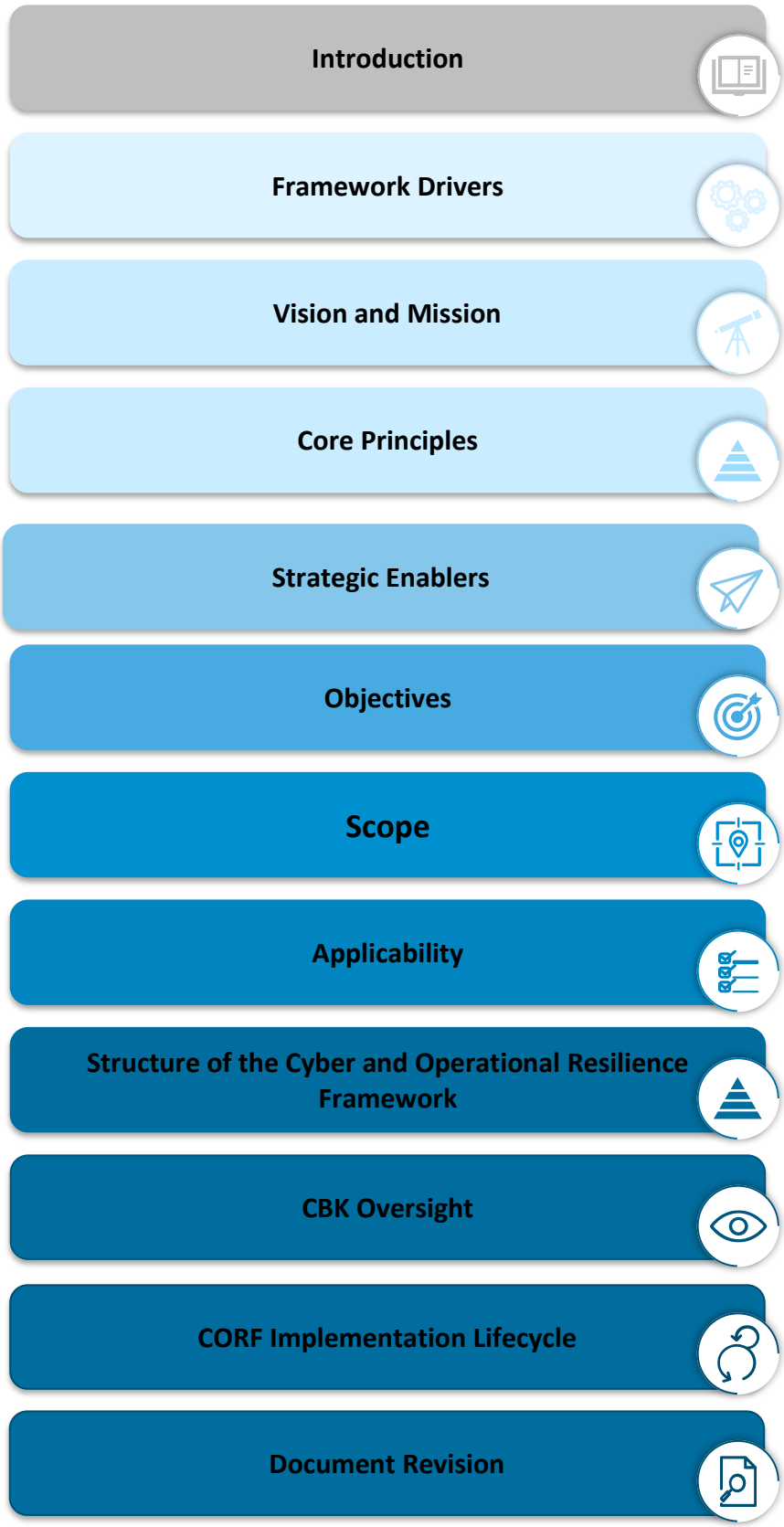
Chapter 1:
Cyber and Operational Resilience Framework

DOCUMENT CONTROL

Date	Version	Author	Change Reference	Reviewer/ Approver
03 Dec 2025	1.0	Central Bank of Kuwait	First Release	Central Bank of Kuwait

TABLE OF CONTENTS

DOCUMENT OVERVIEW



1. Introduction

The Kuwaiti Banking and Financial Sector plays a vital role in maintaining national economic stability, public trust, and ensuring the continuity of essential financial services. As digital transformation accelerates and institutions increasingly rely on interconnected systems, the sector faces a rapidly evolving cyber threat landscape that continue to grow in both scale and sophistication, posing significant risks not only to individual entities, but to the resilience of the entire financial ecosystem.

In this context, building and maintaining cyber and operational resilience has become a strategic imperative, where financial institutions must be prepared not only to protect against cyber threats, but also to anticipate, withstand, recover from, and adapt to adverse situations, ensuring operational continuity and safeguarding the confidentiality and integrity of the financial system.

Pursuant to Article 15 of Law No. 32 of 1968, which mandates the Central Bank of Kuwait (CBK) to regulate and oversee the banking sector in the State of Kuwait and take the necessary measures to maintain their soundness, the CBK has long prioritized strengthening cyber and information security practices across the sector.

In 2020, CBK issued the Cybersecurity Framework (CSF) to establish foundational controls for managing cyber and information security risks across its Regulated Entities. While the CSF provided a strong foundation and served its purpose effectively at the time, the pace of technological change, emergence of complex advanced threats, and the heightened regulatory expectations at both national and global levels have created the need for a more agile and forward-looking approach.

To address these developments, CBK has evolved the CSF into the Cyber and Operational Resilience Framework (CORF), which is a comprehensive and enhanced successor that reflects a strategic shift to a resilience-driven model. The CORF builds on the foundation set by the CSF and is designed to help the Regulated Entities strengthen their cyber capabilities, align with internationally recognized standards and global directions, and adapt to the evolving risk landscape while supporting national objectives.

2. Framework Drivers

The development of the CORF has been driven by the increasing need to strengthen cybersecurity and operational resilience across the sector in response to evolving threats, technologies, and regulatory priorities. The framework builds on the foundation of the 2020 CSF, by adopting a more forward-looking, adaptive, and comprehensive approach. Key drivers include:

- **Regulatory Mandate and Supervisory Responsibility** - In line with CBK Law No. 32 of 1968 and Law No. 20 of 2014, CBK initiates necessary measures to ensure the soundness, stability, and resilience – including in the face of cyber risks across the Kuwaiti Banking and Financial Sector.
- **Escalating Cyber Threats** – Cyber-attacks are growing in frequency, complexity, and systemic impact, posing risks to financial stability, customer trust, and operational continuity.
- **Emerging Sector Needs** – As new operational realities and technologies have emerged, necessitating more adaptive, scalable, and resilience-oriented framework that can address emerging risks, sector interdependencies, and advanced technology adoption.
- **Accelerated Digital Transformation** – The widespread and rapid adoption of cloud computing, Artificial Intelligence (AI), Machine Learning (ML), Quantum Computing, and

other emerging technologies, along with regulatory innovative initiatives such as Open Banking and Sandboxing, is reshaping the banking and financial sector, regulated entities, and the wider financial ecosystem.

- **Expanded Third-Party and Supply Chain Exposure** – Increasing reliance on outsourcing, FinTech partnerships, and interconnected service providers amplifies risk complexity and demands strengthened third-party oversight and control assurance.
- **Alignment with International Standards and Evolving Global Expectations** – International regulators and standardization bodies are placing greater emphasis on sector-wide operational resilience, consistent control implementation, and regulatory accountability.
- **Shift Toward a "Safe-to-Fail" Mindset** – Recognizing that no system is immune to disruption, the CORF promotes the design of secure environments that are resilient by default; able to absorb, recover from, and adapt to cyber incidents with minimal impact on critical operations and the broader sector.
- **Support for National Strategic Objectives** – The CORF contributes to the realization of Kuwait Vision 2035 by enabling the secure and resilient delivery of digital financial services, reinforcing public confidence, and supporting the broader goals of digital transformation and economic diversification.
- **Need for National Consistency and Sector-Wide Coordination** – Disparate cybersecurity approaches can create systemic gaps. A unified framework promotes shared standards, enhanced visibility, and improved cross-institutional response readiness.

3. Vision and Mission

3.1 Vision

To maintain a resilient, secure, and trusted ecosystem of the Banking and Financial Sector and Regulated Entities in Kuwait that is capable of effectively and proactively managing cyber and operational risks, adapting to emerging threats, and sustaining confidence in the digital economy, while positioning CBK as a regional and international leader in cyber and operational resilience and supervisory excellence, and as a benchmark for regulatory effectiveness in cyber and operational resilience advancement.

3.2 Mission

To strengthen the cyber and operational resilience of CBK Regulated Entities by providing a structured framework that promotes consistent cybersecurity and resilience practices, sector-wide coordination, and informed regulatory oversight, executed with excellence, agility, and global competitiveness that reinforces Kuwait's strategic edge in the evolving digital financial landscape.

3.3 Lifecycle

Considering the evolving digital and technology landscape, the CORF is designed and developed accounting for frequent revisions and updates. CBK will evaluate the need for any updates and take the necessary actions to ensure continued relevance amid evolving threats, technologies, and regulatory developments.

4. Core Principles

The CORF is underpinned by a set of core principles that guide its structure and implementation. These principles reflect CBK's regulatory philosophy and establish the foundational approach to strengthening cyber and operational resilience across the sector. The core principles of this framework are as follows:

- **Resilience-First and Threat-Led Approach** – The CORF emphasizes anticipating, withstanding, recovering from, and adapting to cyber threats through threat-led assessments and resilient by design practices.
- **Proportionality and Relevance** – Implementation of the CORF is tailored to each Entity's context, ensuring proportional alignment with size, complexity, and exposure.
- **Tiering-Based Supervisory Oversight** – A structured tiering mechanism enables CBK to conduct proportionate and risk-informed oversight based on Entity's inherent risk profile.
- **Accountability and Governance** – The CORF places ultimate accountability for cyber and operational resilience on the Board of Directors and Executive/Senior Management to drive governance and strategic oversight.
- **Alignment with International Standards and Best Practices** – The CORF aligns with internationally recognized standards and best practices, while reflecting Kuwait's specific regulatory and operational environment.
- **Innovation-Driven and Forward-Looking Design** – Designed for adaptability, the CORF fosters innovation and Research and Development (R&D) to keep pace with emerging technologies and evolving threats.
- **Common Baseline and Sector-Wide Alignment** – A unified baseline ensures consistent expectations, regulatory oversight, and collective sectoral resilience.
- **Continuous Maturity and Capability Improvement** – The CORF encourages Entities to progress beyond baseline to advanced and innovative practices through continuous validation and improvement.
- **Human Capital as a Resilience Foundation** – Cyber and operational resilience depends on a sufficient and skilled workforce, reinforcing human capital as a critical national asset.
- **Collaborative Ecosystem and Community Integration** – The CORF promotes sector-wide collaboration, integration with national entities like the National Cybersecurity Center (NCSC), and alignment with CBK's strategic initiatives.

5. Strategic Enablers

The successful implementation of the CORF depends not only on defined requirements, but also on key enablers that support effective execution, continuous improvement, and sector-wide alignment. These enablers strengthen the overall impact of the framework by fostering the conditions necessary for measurable and sustainable resilience. The strategic enablers of the CORF includes:

- **Sector-Wide Coordination and Engagement** - Strengthening collaboration across Regulated Entities to promote shared understanding, consistent implementation, and collective preparedness.
- **Effective Information Sharing** - Enhancing the timely exchange of threat intelligence, incident insights, and good practices to improve detection, response, and recovery capabilities across the sector.
- **Cyber Resilience Workforce Development** - Translating the strategic priority of human capital into sustained action by investing in the recruitment, development, and retention of skilled cybersecurity professionals at all levels.
- **Measurement and Benchmarking** - Leveraging structured assessment criteria, indicators, metrics, and benchmarking to monitor implementation, track progress, drive accountability, and inform regulatory oversight.
- **Automation** – Encouraging the adoption of advanced cybersecurity tools, automation platforms, and analytics to improve control effectiveness, operational efficiency, risk visibility, and enable timely risk mitigation.

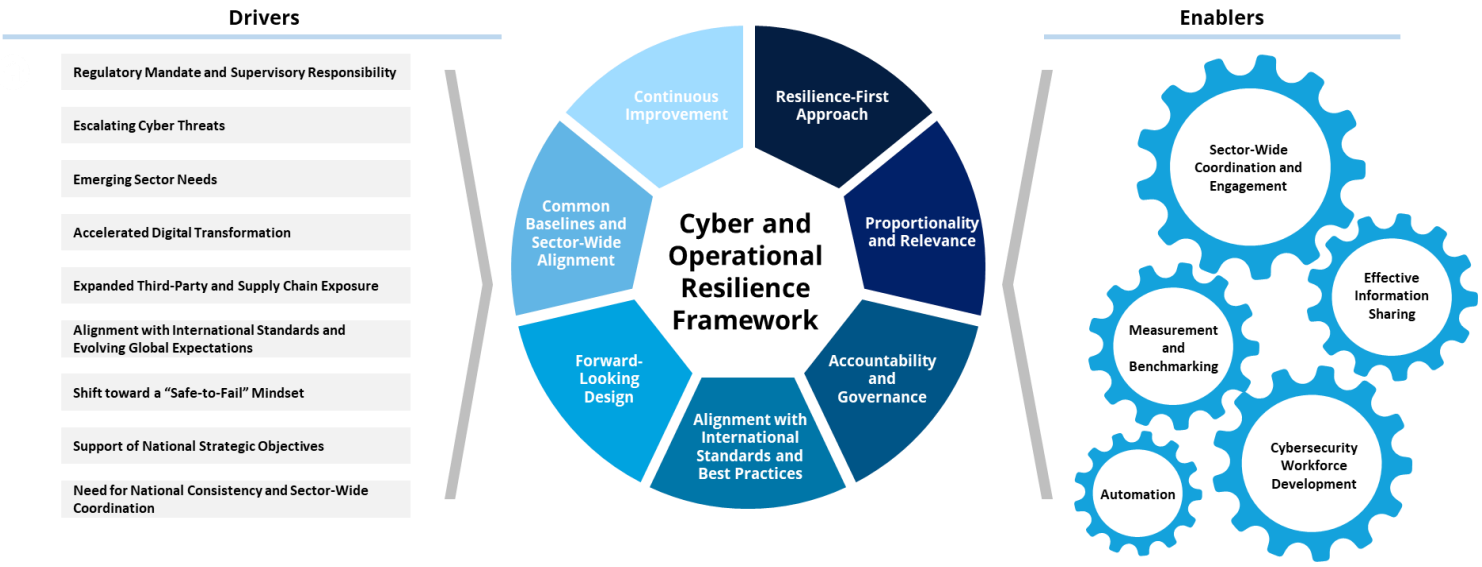


Figure 1. Cyber and Operational Resilience Framework (CORF)

6. Objectives

The main objectives of the CORF are depicted in Figure 2 below:

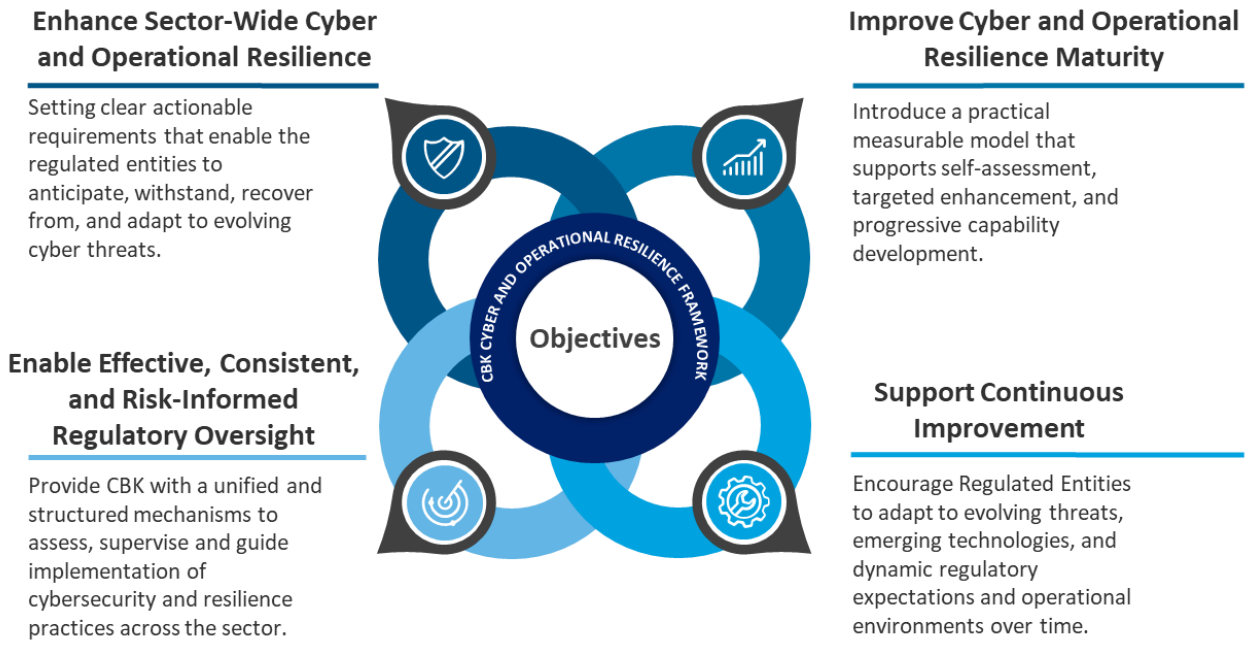


Figure 2. CORF Objectives

7. Applicability

This framework applies to all Regulated Entities under the supervision of CBK.

8. Structure of the Cyber and Operational Resilience Framework

The CORF is structured as a comprehensive and modular regulatory framework composed of interrelated chapters. Together, these chapters define the expectations and guidance necessary to strengthen cyber and operational resilience across CBK Regulated Entities.

9. Scope

The CORF sets the foundational expectations for managing cyber and operational resilience and information security across CBK Regulated Entities, which intends to strengthen the resilience of individual Regulated Entities while contributing to the overall stability, security, and resilience of the sector.

The scope of the framework includes:

- Establishing baselines for the protection of systems, data, and services.
- Embedding resilience principles across governance, technology, and operational layers.
- Addressing risks arising from digital transformation, third-party dependencies, and the adoption of emerging technologies.

- Supporting the development of cyber resilience workforce capabilities across the sector.
- Promoting sector-wide alignment and regulatory oversight through a unified set of control requirements.

9.1 Framework

The Framework is the overarching high-level reference for the CORF, issued by CBK to define the strategic vision, mission, and regulatory expectations for enhancing cybersecurity and resilience across the sector.

This document sets out the CORF's purpose, scope, core principles, and structural taxonomy. It outlines the obligations of the Regulated Entities and establishes the oversight role of CBK. It anchors the CORF and brings together its core components "CORWG TOR, Baselines, and CORF Toolkit", explaining the purpose of each component, providing a unified view of how the CORF to be interpreted. It is informed by key drivers and supported by enablers that promote cyber and operational resilience across the sector.

9.2 Cyber and Operational Resilience Working Group Terms of Reference (CORWG TOR)

This chapter outlines the mandate, composition, and functioning of the Cyber and Operational Resilience Working Group (CORWG), which serves as a forum established by CBK for sector-wide coordination.

The CORWG enables collaboration between CBK and Regulated Entities on evolving cyber threats, regulatory initiatives, incident learnings, and the continuous improvement of the cybersecurity and resilience capabilities across the sector. The TOR outlines the working group's governance structure, membership, roles and responsibilities, meeting frequencies, communication protocol, and documentation management.

9.3 CORF Toolkit

The CORF Toolkit is the primary tool for Regulated Entities adopting the CORF. While the rest of CORF documents outline the "what", the Toolkit provides clarity on the "how". It offers structured guidance, standardized templates, and reference materials to ensure effective application of CORF requirements. The Toolkit comprises of four key components.

9.3.1 Assessment Criteria Guidelines

The assessment criteria have been revamped to introduce a dual-layered assessment methodology that ensures a more objective and structured evaluation process. It enables CBK to monitor both compliance and maturity progress across the sector.

a. **Control-Level Compliance Assessment** – Each control in the Baselines document is assessed as either Compliant, Non-Compliant, or Not Applicable (where formally justified by the Regulated Entity and approved by CBK), based on documented verifiable evidence. This binary assessment ensures uniformity and accountability in compliance tracking, and promotes a clear and enforceable compliance posture, avoiding partial or subjective interpretations. Compliance percentages will be rolled-up at the control area level.

b. **Sub-Domain Level Maturity Assessment** – Each sub-domain is assessed against a standardized five-level maturity scale (1- Initial, 2- Ad-hoc, 3- Baseline, 4- Advanced, 5-

Innovative) to evaluate the extent to which Regulated Entities have institutionalized and optimized their cybersecurity and resilience practices and capabilities. This model is progressive in nature, meaning that advancement to higher levels requires full and demonstratable achievement of the preceding one, ensuring that improvements are meaningful and sustainable.

The five levels reflect the increasing depth, integration, process consistency, optimization, and effectiveness of cybersecurity and resilience capabilities within an entity. Maturity attributes have been defined per sub-domain to guide assessors, ensure assessments are aligned with expected practices at each level, and support meaningful benchmarking and improvement. Figure 3 illustrates the five maturity levels and their definitions.

c. **Domain Level Compliance and Maturity** – For each domain, the compliance percentages are rolled-up to the domain level to come up with the domain compliance score. Similarly, the maturity level is determined by averaging the maturity scores of all its associated sub-domains. This would provide a balanced representation of domain-level resilience, accounting for the breadth and capabilities implemented across its sub-domains.

d. **Overall Cyber Maturity Level of the Regulated Entity** – Calculated by averaging the maturity levels of all domains, offering a consolidated view of the Entity's cyber and operational resilience posture.

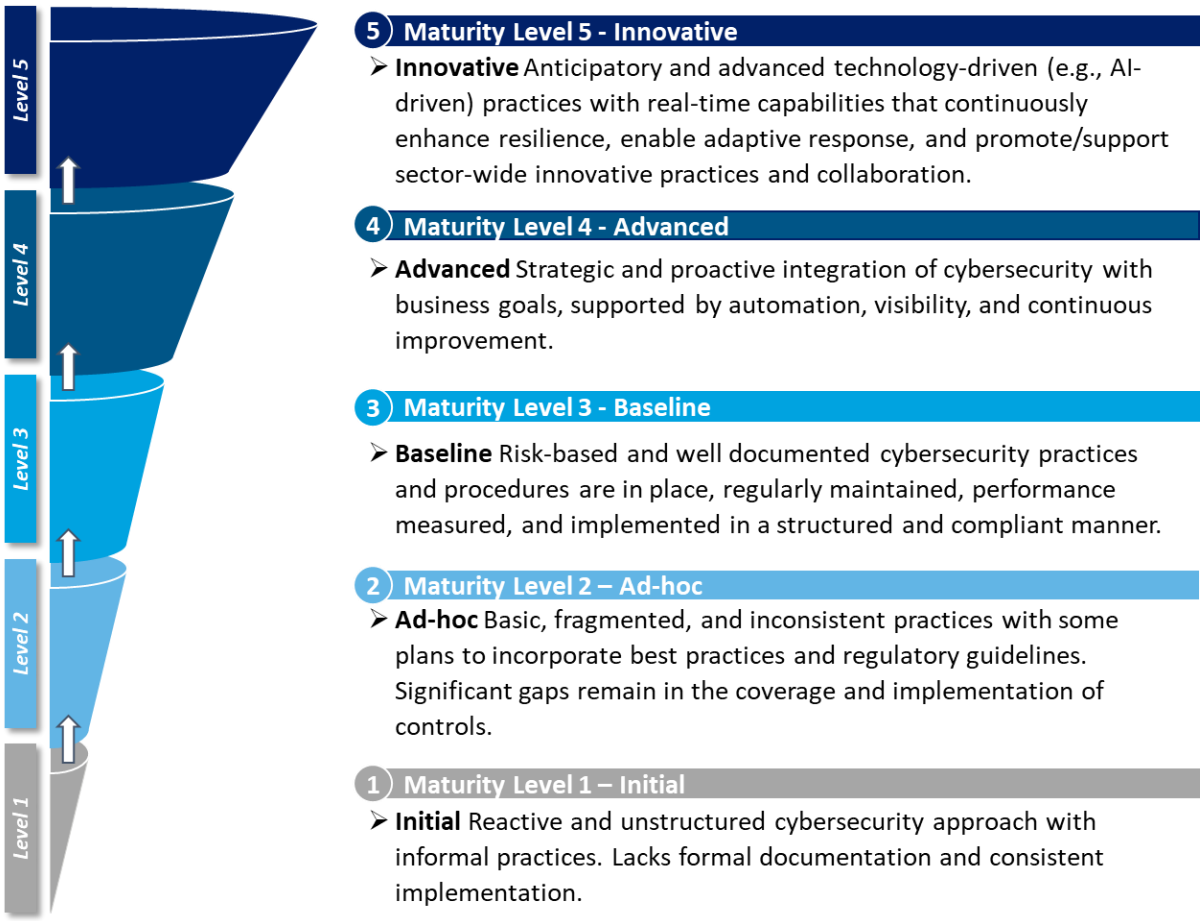


Figure 3. Cyber and operational Resilience Maturity Levels

9.3.2 Statement of Applicability (SoA)

The CORF Toolkit document includes a standardized Statement of Applicability (SoA) template along with accompanying guidance to support its consistent completion and use across the Regulated Entities. The aim of reporting the SoA is to act as a formal declaration of which domains and sub-domains within the CORF are applicable to the Entity, based on its business model and services provided.

Regulated Entities are required to complete and submit the SoA to CBK ahead of any CORF assessment or audit. Where domains and/or sub-domains is deemed not applicable, the Entity must provide a clear and well-justified reasoning, which will be subject to CBK review and formal approval.

9.3.3 Cyber Resilience Workforce Management

The CORF Toolkit document includes the Cyber Resilience Workforce Framework (CRWF), which establishes a comprehensive sector-wide approach to developing and sustaining cybersecurity talent across the sector. The CRWF addresses the growing demand for skilled professionals by providing structured guidance on workforce development, role definition, capability building, and long-term resilience.

The CRWF consists of three key parts:

a. Job Categories, Job Roles, Required Skills, and Qualifications – This outlines key cybersecurity job categories, roles, required skills, and qualification benchmarks tailored to the banking and financial sector and other CBK Regulated Entities. It provides a foundation for standardized workforce planning, recruitment, and capability development across the Entities.

b. Senior Cybersecurity Leadership Program (SCLP) – Designed to equip executives and decision-makers with the mindset, strategic skills, and governance awareness required to lead in an increasingly complex cyber threat environment. The program aligns with national security goals and supports coordinated leadership development across the sector.

c. Cybersecurity Resilience Assessor Program (CRAP) – Prepares cyber auditors, CBK teams, and independent assessors with the practical and regulatory expertise needed to evaluate compliance with the CBK CORF, PCI-DSS, ISO27K and other relevant international standards, best practices, global and regional banking regulations. It promotes consistency and regulatory alignment in sector-wide assessments.

Together, these programs reinforce a unified, capable, and forward-looking cyber resilience workforce necessary for the effective implementation and maintenance of cybersecurity and resilience measures.

9.3.4 Inherent Risk Profiling

The CORF Toolkit document includes inherent risk profiling that forms a foundational component designed to enable CBK to determine the appropriate tier classification for each Regulated Entity based on its underlying inherent risk exposure. Through a structured set of inputs mapped to defined tiering dimensions outlined in Section 10 of this Framework document, Entities provide information reflecting their operational scale, service delivery model, technology environment, and overall risk posture, supplemented by limited number of supervisory-specific inputs from CBK. This profiling supports a proportionate and risk-based oversight model by informing the scope, frequency, and intensity of supervisory activities and engagement, while also enhancing visibility into systemic risks across the sector.

9.3.5 Circulars

The CORF Toolkit document includes list of circulars issued by the CBK to provide guidelines, instructions and updates to the CBK Cyber and Operational Resilience Framework. These circulars serve to clarify and provide specific regulatory requirements with the aim to strengthen the resilience of the banking and financial sector against cyber threats. Compliance with these circulars is mandatory to all Regulated Entities.

9.4 Cyber Resilience Baselines

The Cyber Resilience Baselines defines the foundational controls and minimum requirements that Regulated Entities are expected to implement under the CORF. It operationalizes the framework's strategic approach to concrete and measurable controls that strengthen both Entity-level and sector-wide cyber resilience.

The Cyber Resilience Baselines follows a four-level hierarchical structure: individual controls that are grouped into control areas, which are organized under relevant sub-domains, all of which are mapped to overarching domains. The Cyber Resilience Baselines comprises of (6) Domains, (33) Sub-Domains, (87) Control Areas, and (519) Controls:

Domain 1 – Governance, Risk, 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 applicable global and local compliance requirements. It constitutes of (5) sub-domains:

Domain	Governance, Risk, and Compliance		
Sub-Domains	Cyber Resilience Governance and Oversight	Cybersecurity Risk Management	Compliance
	Independent Audit	Workforce Management	

Domain 2 – 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. Technology and Operations domain comprises (16) sub-domains:

Domain	Technology and Operations		
Sub-Domains	Security Architecture Design	Asset Management	Infrastructure and Network Security
	Endpoint and Device Security	Email Security	Identity and Access Management
	Cryptography	Application Security and Secure SDLC	Change and Release Management

Domain	Technology and Operations		
	Capacity Management	Data Protection and Privacy	Logging, Monitoring, and Security Incident Management
	Cybersecurity Testing and Threat Management	Physical and Environmental Security	Cyber Threat Intelligence
	Digital Risk Protection		

Domain 3 – Third-Party Risk Management and Supply Chain Management

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. It has (2) sub-domains:

Domain	Third-Party Risk Management and Supply Chain Management	
Sub-Domains	Third-Party Risk Management (TPRM)	Supply Chain Management

Domain 4 – Emerging Technologies

This domain defines the controls and security considerations for emerging technologies such as Artificial Intelligence (AI), Machine Learning (ML), blockchain, and cloud computing. This shall help Regulated Entities to identify, mitigate and effectively manage risks related to emerging technologies. It includes (2) sub-domains:

Domain	Emerging Technologies	
Sub-Domains	Advanced Technologies Security	Cloud Security

Domain 5 – Payments Security

This domain defines the baselines that shall be implemented by the Regulated Entities to identify, mitigate, and monitor cybersecurity risks related to payment systems. It is comprised of (6) sub-domains:

Domain	Payments Security		
Sub-Domains	Common Security Controls for Electronic Payment Systems	Electronic Payment Transactions Monitoring	Digital Banking Security
	Payment Card Data Security	Security of Customer Self-Service Machines	Contactless Payment Technology Security

Domain 6 – Operational Resilience

This domain outlines the controls related to business continuity, disaster recovery and crisis management, including the requirements for developing, maintaining, and effectively monitoring cyber resilience efforts. This will help Regulated Entities identify and effectively manage risks related to cyber resilience. Operational Resilience domain is made up of (2) sub-domains:

Domain	Operational Resilience	
Sub-Domains	Business Continuity and Disaster Recovery (BC and DR)	Cyber Crisis Management

9.5 Operational Resilience Baselines

The Operational Resilience Baselines (ORB) form an integral component of the CORF, defined to complement and support its implementation. The ORB establishes the foundational controls and minimum requirements that Regulated Entities are expected to implement to enhance their ability to anticipate, withstand, respond to, and recover from disruptions, thereby strengthening both Entity-level and sector-wide operational resilience.

The Operational Resilience Baselines document follows a four-level hierarchical structure: individual controls that are grouped into control areas, which are organized under relevant sub-domains, all of which are mapped to overarching domains. This comprises of (8) Domains, (17) Sub-Domains, (35) Control Areas, and (146) Controls:

Domain 1 – Governance and Oversight

This domain shall establish a structured governance framework, to ensure accountability and alignment with regulatory requirements. This will help oversee the implementation of operational resilience across the Regulated Entity. It constitutes of (3) sub-domains:

Domain	Governance and Oversight		
Sub-Domains	Operational Resilience Governance Structure and Oversight	Operational Resilience Policy and Strategy	Compliance

Domain 2 – Risk and Threat Management

This domain shall enable the identification, assessment, and evaluation of business disruption risks and continuous monitoring, to support proactive mitigation and informed decision-making. This will help the Regulated Entity apply standardized methodologies to manage and treat risks. Risk and Threat Management domain comprises (3) sub-domains:

Domain	Risk and Threat Management		
Sub-Domains	Risk Assessment Methodology	Risk Assessment Process	Risk Treatment and Reporting

Domain 3 – Business Continuity Management

This domain shall define business continuity strategies and plans, to sustain critical business functions during and after disruptions. This will help the Regulated Entity ensure preparedness for service restoration under various disruption scenarios. The domain is made up of (3) sub-domains:

Domain	Business Continuity Management		
Sub-Domains	Business Impact Analysis	Recovery Strategies	Business Continuity Plans (BCP)

Domain 4 – Technology Resilience

This domain shall define the recovery and restoration mechanisms for critical IT systems and infrastructure, to ensure timely resumption of technology services. This will help the Regulated Entities align technology recovery planning with business requirements. The domain constitutes of (5) sub-domains:

Domain	Technology Resilience		
Sub-Domains	Service Management	Backup and Recovery Management	Technology and Resilience Capabilities
	Technology Recovery Plans	Cyber Recovery Plans	

Domain 5 – Third-Party Resilience

This domain shall establish requirements for third-party service providers, to maintain continuity of externally delivered critical services. This will help the Regulated Entity assess, monitor, and manage third-party risks. This domain links to the TPRM Baselines, where Entities shall refer to Domain 5 of TPRM Baselines within the CORF.

Domain 6 – Incident and Crisis Management

This domain shall define structured response processes for managing incidents and crises, to enable timely detection, escalation, and resolution of disruptive events. This will help the Regulated Entity coordinate recovery actions and reduce operational impact. Incident and Crisis Management domain contains (2) sub-domains:

Domain	Incident and Crisis Management	
Sub-Domains	Incident and Crisis Management Governance and Planning	Communication and Escalation

Domain 7 – Cyber Resilience

This domain shall implement controls that enable the Regulated Entity to recover from cyber incidents and continue critical operations with minimal disruption. This will help the Regulated Entity maintain operational continuity and resilience in the face of evolving cyber threats. This domain links to CBK Cyber Resilience Baselines, where Entities shall refer to Domain 9 of the Cyber Resilience Baselines under the CORF.

Domain 8 – Testing, Training, and Continuous Improvement

This domain shall establish mechanisms for validation, awareness, and review, to enhance preparedness and embed resilience culture and drive continuous improvement. This will help the Regulated Entity improve resilience capabilities through continuous learning and testing. This domain has (1) sub-domain:

Domain	Testing, Training and Continuous Improvement
Sub-Domain	Training, Testing and Exercising

9.6 Third-Party Risk Management Baselines

The Third-Party Risk Management (TPRM) Baselines are a dedicated component of the CORF, established to reinforce its implementation. The TPRM Baselines define the foundational controls and minimum requirements that Regulated Entities are expected to implement to ensure the effective identification, assessment, monitoring, and management of risks arising from third-party relationships and supply chain dependencies.

The Third -Party Risk Management Baselines document follows a four-level hierarchical structure: individual controls that are grouped into control areas, which are organized under relevant sub-domains, all of which are mapped to overarching domains. This comprises of (13) Domains, (43) Sub-Domains, (78) Control Areas, and (211) Controls:

Domain 1 – Governance Structure and Oversight

This domain shall enable Regulated Entities to establish a robust framework for Third-Party Risk Management (TPRM), aligning policies and strategies with organizational goals and regulatory requirements. It fosters accountability, strategic oversight, and continuous improvement through clear roles, rigorous approvals, and periodic reviews, enhancing resilience against evolving risks. The domain is comprised of (4) sub-domains:

Domain	Governance Structure and Oversight		
Sub-Domains	TPRM Policy and Strategy	Roles and Responsibilities	Board and Senior Management Oversight
	Approvals and Periodic Review		

Domain 2 – Risk Management Framework

This domain shall ensure effective management of third-party risks by identifying critical services, assessing risks across multiple dimensions, and mapping dependencies to enhance operational resilience and inform business continuity planning. It constitutes of (3) sub-domains:

Domain	Risk Management Framework		
Sub-Domains	Critical Third-Party Service Identification	Risk Identification and Assessment Methodology	Dependency Mapping to Critical Processes

Domain 3 – Contractual Agreements Considerations

This domain outlines the foundational legal, regulatory, and governance expectations that shall be embedded within third-party contractual arrangements. It ensures that Regulated Entities maintain enforceable agreements that support operational resilience, regulatory compliance, and risk mitigation across all third-party engagements. These provisions are critical to ensuring service continuity, accountability, and oversight during normal operations and disruption scenarios. This domain is made up of (7) sub-domains:

Domain	Contractual Agreements Considerations		
Sub-Domains	Contractual Safeguards	Legal Binding Agreement	Regular Monitoring and Assessment
	Health Safety and Environment	Financial Viability	Compliance (Geopolitics, Regulatory, Organizational, Country and Legal)
	Corporate Governance		

Domain 4 – Risk Assessment and Monitoring

This domain shall define establishing a robust process for the systematic identification, assessment, and continuous monitoring of risks—particularly those impacting critical IT systems and business operations. The domain includes (3) sub-domains:

Domain	Risk Assessment and Monitoring		
Sub-Domains	Identification, Assessment, and Mitigation	Risk Classification	Ongoing Monitoring of Critical Third Parties

Domain 5 – Business Continuity Management and Disaster Recovery

This domain shall establish requirements for third-party service providers, to maintain continuity of externally delivered critical services. This will help Regulated Entities assess, monitor, and manage third-party resilience capabilities. It includes (5) sub-domains:

Domain	Business Continuity Management and Disaster Recovery		
Sub-Domains	Business Continuity Plans	Data Backup and Replication	Periodic Testing of DR Capabilities
	Recovery and Restoration Procedures	Business Continuity Management and Recovery	

Domain 6 – Incident Management

This domain shall establish requirements for third-party incident management, ensuring effective detection, response, and resolution to enhance security and resilience. Incident Management domain has (3) sub-domains:

Domain	Incident Management		
Sub-Domains	Incident Detection and Monitoring	Incident Communication and Escalation Protocols	Root Cause Analysis

Domain 7 – Data Protection and Confidentiality

This domain shall define third-party data management practices to maintain ensure data security and compliance, protecting sensitive data throughout its lifecycle. The domain constitutes of (3) sub-domains:

Domain	Data Protection and Confidentiality		
Sub-Domains	Data Encryption and Masking	Data Retention and Disposal	Data Classification and Handling Policies

Domain 8 – Sub-Contracting

This domain shall ensure third-party sub-contracting arrangements are disclosed and approved, maintaining oversight and control to adhere to vendor risk management policies and mitigate associated risks. It includes (2) sub-domains:

Domain	Sub-Contracting	
Sub-Domains	Disclosure of Subcontractor and Approval from Regulated Entities	Monitoring and Oversight

Domain 9 – Exit Strategy

This domain shall ensure Regulated Entities implement proper exit strategies for third-party engagements, to maintain service continuity and data security. The domain has (1) sub-domain:

Domain	Exit Strategy
Sub-Domain	Exit Strategy Planning

Domain 10 – Storage of Data

This domain establishes the protection measures of sensitive data through secure storage practices, supporting compliance and resilience against data loss and unauthorized access. This domain is made up of (3) sub-domains:

Domain	Storage of Data		
Sub-Domains	Data Storage Security	Storage Lifecycle Management	Data Integrity and Availability

Domain 11 – Cross-Border Transaction

This domain shall establish compliance measures for cross-border transactions, ensuring adherence to legal, regulatory, and privacy requirements to mitigate risks and uphold financial integrity. Cross-Border Transaction domain constitutes of (4) sub-domains:

Domain	Cross-Border Transaction		
Sub-Domains	Regulatory and Legal Compliance	Due Diligence and KYC/AML	Secure Data Transfers and Privacy
	Monitoring, Reporting, and Audit		

Domain 12 – Usage of Cloud Services

This domain shall ensure Regulated effectively manage the risks associated with cloud service providers, ensuring compliance across jurisdictions, and maintaining cloud security, which is crucial for safeguarding data. This domain includes (1) sub-domain:

Domain	Usage of Cloud Services
Sub-Domain	Cloud Security

Domain 13 – Inter-Affiliates

This domain shall establish the requirements for managing affiliate engagements in an effective way to uphold compliance, mitigate risks, and maintain services continuity. The domain includes (4) sub-domains:

Domain	Inter-Affiliates		
Sub-Domains	Due Diligence and Periodic Review	Customer Consent	Foreign Affiliates
	Resource Planning		

10.CBK Oversight

Under its supervisory mandate, CBK plays a central role in overseeing the implementation of the CORF across all Regulated Entities. CBK's oversight ensures that entities align with and adhere to the expectations outlined in the CORF, implement the required controls, and maintain a state of preparedness to respond to and recover from cyber incidents.

This oversight function is not limited to enforcements, it is also fundamental to protecting the integrity of the national financial system and fostering sector-wide cyber and operational resilience.

10.1 Risk-Based Tiering Approach

To ensure proportionate and effective supervision, CBK applies a structured risk-based tiering model to categorize Regulated Entities based on their systemic importance, operational complexity, and overall cyber risk exposure. This approach allows CBK to calibrate the scope, depth, and frequency of oversight activities according to the relevant impact an entity could have on national financial stability and sector-wide resilience.

The adopted tiering approach acknowledges that not all entities present the same level of risk or require the same depth of engagement. It supports prioritization of supervisory engagements, differentiated expectations based on risk, and enhanced visibility into entities with significant operational interdependence or systemic roles.

10.1.1 Tiering Dimensions and Criteria

CBK determines tier placement through an assessment of each Regulated Entity's risk profile, drawing from a combination of quantitative metrics and qualitative risk indicators. This ensures that tiering is both evidence-based and reflective of the entity's current and potential impact on the national financial resilience.

The following dimensions are considered in determining tier classification:

- **Total Number of Assets** – Reflects the financial scale of the entity and its potential impact on the overall stability of the sector.
- **Market Share** – Indicates the entity's dominance or influence within the respective financial segment (e.g., deposits, loans, digital payments).
- **Branch Network and Channels** – Evaluates the geographic spread and delivery mechanisms (e.g., physical branches, neobanks, mobile applications, ATMs/ITMs) that contribute to the entity's exposure and operational footprint.
- **Customer Base** – Considers the size and diversity of the customer population served, and the potential impact of service disruption.
- **Nature and Breadth of Services** – Assesses whether the entity provides retail banking, corporate banking, investment, financing, or payment services, including digital and cross-border offerings.
- **Infrastructure Role** – Includes designation as an FMI, such as operators of payment gateways, credit information networks, or other essential platforms.
- **Technological Complexity** – Covers the extent of emerging and advanced technologies usage, such as Cloud adoption, use of APIs, AI/ML, and integration with digital platforms.
- **Outsourcing and Third-party Dependencies** – Evaluates the level of interconnectivity with third-parties and reliance on outsourcing.

- **Cyber Risk Exposure and Threat Landscape** – Involves the attack surface introduced by digital transformation, legacy systems, or public-facing systems/platforms.
- **Regulatory and Supervisory History** – Considers CBK's previous audit findings, cyber incidents that revealed material weaknesses in cybersecurity and resilience posture, and responsiveness to regulatory requirements.
- **Cyber Resilience Workforce –** Takes into consideration the number of directly attributed personnel working on cybersecurity initiatives to ensure proportionate coverage given potential exposure.

10.1.2 Tiers and Definitions

Based on the tiering dimensions outlined in the previous sub-section, CBK categorizes the Regulated Entities into three main supervisory tiers. This categorization reflects each entity's systemic importance to the overall resilience of the sector.

The tiering is not static; CBK reviews and updates tier assignments periodically, particularly in response to:

- Mergers, acquisition, or re-structuring;
- Rapid growth in digital or operational footprint, customer base, or market share;
- New regulatory requirements or changes in FMI designation;
- Emerging threats or reported cyber incidents; or
- Performance in previous assessments.

Below are the tiers and the definitions per each:

Tier 1 – High-Impact Entities

This includes entities with systemic significance, due to their large asset base, significant market share, extensive customer base, and broad digital operations. Examples of such entities are major domestic banks (aka Domestic Systematically Important Banks (D-SIBs)), large foreign bank branches, and Financial Market Infrastructures (FMIs) that operate national payment, clearing, or settlement systems.

These entities play a critical role in the stability of the sector and are therefore subject to frequent and detailed oversight, given their criticality and sectoral functioning. Entities within this tier shall undergo a CORF assessment by CBK on an annual basis. CBK may engage in more frequent check-ins with these entities and may require participation in thematic reviews, depending on the cyber risk landscape.

Tier 2 – Medium-Impact Entities

This includes mid-sized entities with moderate systemic relevance, substantial market presence, and operational complexity. These entities are subject to CORF assessment by CBK every eighteen months, with additional supervisory touchpoints or thematic reviews based on their evolving risk profile, conducted as needed.

Tier 3 – Low-Impact Entities

This includes entities with limited market share, small customer base, narrow service offerings, and lower cyber risk exposure. These entities are subject to CORF assessment by CBK every two years, unless otherwise triggered by major incidents, emerging risks, or regulatory findings.

10.2 Oversight Activities and Mechanisms

Based on each entity's assigned tier and overall risk profile, CBK conducts a range of oversight activities to verify compliance, assess cyber and operational resilience maturity, and ensure sector-wide alignment with the CORF. The nature and frequency of these activities are tier-calibrated to ensure proportionality while maintaining comprehensive coverage.

CBK's oversight mechanisms may include:

- **Structured Reviews and Assessments** – Periodic examinations of CORF implementation, supporting evidence, and maturity assessments.
- **Thematic Reviews and Deep Dives** – Targeted reviews focused on priority areas, such as third-party risk, Cloud security, digital payment resilience, or data protection and privacy.
- **Spot Checks** and **Ad-hoc Reviews** – Reactive or investigative engagements based on emerging threats, incident reports, or intelligence received.
- **Assessment Quality Assurance** – Review of self-assessments and independent assessments submitted by Regulated Entities.

Entities in Tier 1 are subject to more frequent and comprehensive oversight activities, while Tier 2 and Tier 3 follow progressively lighter supervisory cycles, though no tier is exempted from CBK's authority to request documentation or launch ad-hoc reviews at any time.

Oversight is supported through CBK internal capabilities as well as sectoral coordination forums such as the CORWG, ensuring unified interpretation of CORF obligations and continuous regulatory alignment.

10.3 Sectoral Coordination and Continuous Improvement

In addition to entity-specific oversight, CBK plays a vital role in facilitating sector-wide coordination, knowledge-sharing, and continuous improvement of cybersecurity and resilience practices. Through structured channels and regulatory initiatives, CBK promotes alignment, collaboration, and readiness across all Regulated Entities. Key mechanisms include:

- **Cyber and Operational Resilience Working Group (CORWG)** – A forum chaired by CBK and composed of cybersecurity representatives from Regulated Entities. The CORWG meets quarterly – or more frequently – to discuss emerging threats, regulatory initiatives, incident learnings, and shape sectoral cyber and operational resilience capabilities and response strategies.
- **Sector-Wide Simulations and Exercises** – CBK may initiate cyber crisis simulation drills, threat scenario planning, or business continuity exercises to test collective preparedness and identify systemic weaknesses.
- **Regulatory Guidance and Thematic Reports** – Development and dissemination of advisories, Frequently Asked Questions (FAQs), and thematic reports to clarify expectations and highlight good practices observed during supervisory activities.
- **Workforce and Capacity Building Programs** – CBK supports the upskilling and specialization across the sector through initiatives, fostering a skilled and capable cyber resilience workforce.

Through these efforts, CBK ensures the CORF remains a living framework; one that evolves with emerging threats and risks, supports national cybersecurity and resilience goals, and strengthen the

collective ability of the Kuwaiti banking and financial sector and other CBK Regulated Entities to withstand, respond to, and recover from cyber threats.

11.CORF Implementation Lifecycle

The CORF establishes a structured approach that Regulated Entities shall follow to implement, maintain, and continuously improve their cyber and operational resilience capabilities. This lifecycle depicted in Figure 4, operationalize the key components of the CORF into a clear and iterative process. It enables Entities to assess current resilience posture, address identified gaps, report outcomes to CBK, and continuously strengthening capabilities over time. The lifecycle comprises six main steps, supported by CBK's oversight and directions, and underpinned by the foundational enablers defined in this Framework.

The lifecycle begins with the submission of the Inherent Risk Profile and the SoA. The Inherent Risk Profile is required on annual basis, or whenever significant changes occur in the Entity's operational structure, technological landscape, or threat landscape. The SoA, as illustrated earlier in this document, are to be completed and submitted prior to undergoing any assessment against the CORF and serves to define the applicable scope of Baseline controls in alignment with the Entity's specific operational profile.

This is followed by compliance and maturity assessments against the CORF Baselines to determine the extent of controls implementation and the overall resilience maturity levels across relevant applicable sub-domains. Based on the assessment outcomes, Regulated Entities are then expected to identify gaps, prioritize them based on risk and business impact, and develop an actionable remediation plan.

The next phase involves executing the remediation plan to implement the missing or non-compliant CORF Baselines and uplift maturity levels in line with regulatory expectations. Upon implementation, Entities are required to formally submit the assessment results to CBK, along with the latest and up-to-date inherent risk profile, for their review and oversight.

The lifecycle is designed to be iterative, with periodic reviews and re-assessments, reinforcing the commitment to continuous improvement. Through this cyclical process, Entities strengthen their resilience posture over time and align with evolving regulatory and sectoral expectations.

CBK supports and supervises this process through two core functions; CBK oversight activities as explained in the previous section, and CBK guidance and sectoral initiatives, which encompasses regulatory updates, strategic directions, and coordination of sector-wide efforts, supporting consistent alignment, shared learning, and national resilience objectives.

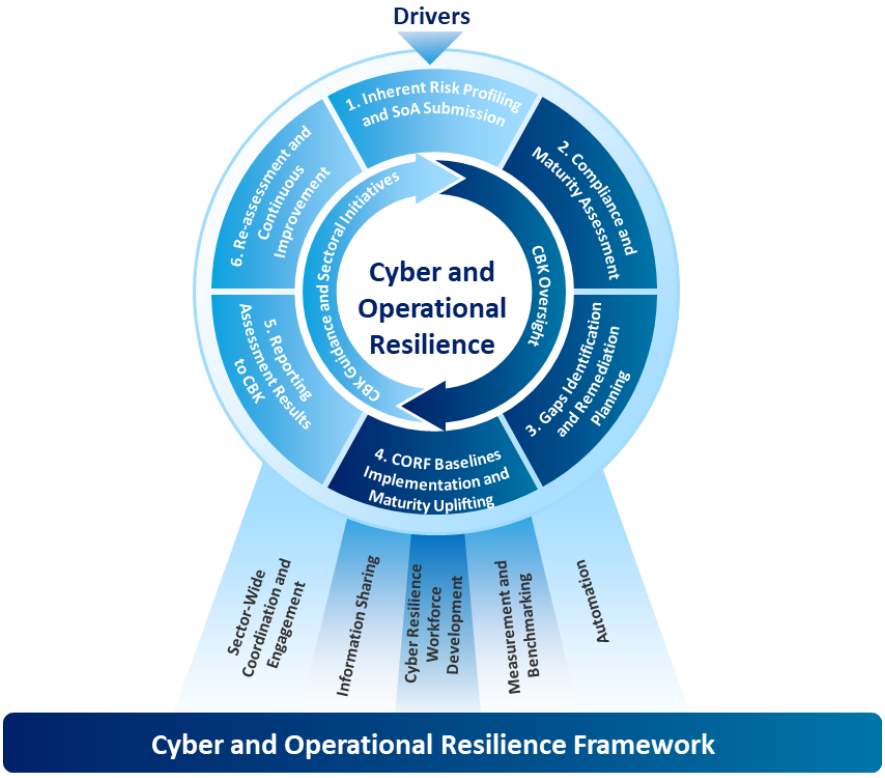


Figure 4. CORF Implementation Lifecycle

12.Document Revision

This document shall be formally reviewed as part of the overall review of the CORF. However, interim updates may be made as deemed necessary by CBK.

Revisions shall be carried out through a structured process led by CBK, in consultation with CORWG and relevant stakeholders. Updates shall be communicated to all Regulated Entities, with clear timelines for implementation.

This approach ensures that the CORF remains current, actionable, and aligned with both national priorities and international standards and best practices, while supporting the continuous improvement of cybersecurity and resilience capabilities across the sector.

Chapter 2:
Cyber and Operational Resilience Working Group Terms of Reference

DOCUMENT CONTROL

Date	Version	Author	Change Reference	Reviewer/ Approver
03 Dec 2025	1.0	Central Bank of Kuwait	First Release	Central Bank of Kuwait

TABLE OF CONTENTS

1. Introduction

As per Article 15 of Law No. 32 of 1968, the Central Bank of Kuwait (CBK) is responsible for supervising the Kuwaiti banking system and safeguarding its soundness and stability. In alignment with this mandate and CBK's expanded supervisory scope covering a broader set of Regulated Entities – including Kuwaiti and Foreign Banks, Exchange Companies, Finance Companies, e-Payment of Funds Companies, Credit Information Companies and Open Banking Service Providers – the CBK has established a formal mechanism to promote collaboration on cyber risk and resilience.

Recognizing the growing complexity and systemic impact of cyber threats, a decision was made by the Central Bank of Kuwait in 2016, to have a dedicated sectoral forum to support information sharing, coordination, and strategic alignment across CBK Regulated Entities. At the time of its formation, the forum was named as the Information Security working Group (ISWG). Since then, ISWG played a pivotal role in shaping and launching the Cybersecurity Framework (CSF) for the Banking and Financial sector back in 2020, laying the foundation for sector-wide cybersecurity practices. Overtime, this initially established ISWG has evolved and expanded considerably in scope and significance. To reflect this evolution, and in alignment with the transition from cybersecurity-focused approach to a broader comprehensive cyber and operational resilience strategy, the group has been formally renamed as the Cyber and Operational Resilience Working Group (CORWG).

This Terms of Reference (hereinafter referred to as 'CORWG TOR' or 'TOR') outlines the purpose, objectives, membership, roles and responsibilities, the code of conduct, communication protocols, and documentation management and version control, of the CORWG. This document forms an integral component of CBK's Cyber and Operational Resilience Framework for CBK Regulated Entities.

2. Purpose

The CORWG is a strategic initiative led by the CBK, to serve as an advisory, alignment, and coordination forum to enhance the cyber and operational resilience of CBK Regulated Entities in Kuwait. The CORWG provides a platform for Regulated Entities and CBK to work collaboratively in identifying, discussing, managing, and mitigating cyber and information security risks, while supporting sector-wide resilience capabilities to prepare for, withstand, respond to, recover from, and adapt to various cyber threats, incidents, and disruptions.

The group enables proactive information sharing, discussions, collective learning, and practical cooperation on key cyber topics, trends, and strategies, thereby contributing to the security, continuity, resilience, and trustworthiness of the banking and financial services in Kuwait.

3. Objectives

The objectives of the CORWG include the following:

a) Provide a formal forum for collaboration, knowledge-sharing, and coordinated action (e.g., shared initiatives, joint planning, and sector-wide responses) to strengthen cyber and operational resilience across CBK Regulated Entities.
b) Facilitate informed dialogue and discussions on emerging cyber and information security threats, latest trends, evolving technologies, and resilience strategies.
c) Advise on sector-wide cybersecurity and resilience initiatives, and provide support and guidance on compliance with applicable regulations and sectoral expectations.
d) Support coordinated preparedness, monitoring, and response to cyber threats and incidents.
e) Participate in sector-wide cyber simulation exercises and maintain coordination with related working groups to ensure alignment of resilience and response efforts.

f) Engage with relevant government entities and external stakeholders to align sectoral efforts with the national cybersecurity and resilience objectives.
g) Promote cybersecurity awareness and build capabilities through joint programs, sector-wide initiatives, and workforce development efforts.

4. CORWG Members

The CORWG is composed of representatives from the regulated entities, as well as CBK itself. The following outlines the composition, eligibility criteria, and participation rights of CORWG members:

a) The CORWG Chairman is to be appointed by H.E. the Governor.
b) The Deputy Chairman, Secretariat, and CBK representatives shall be nominated by the CORWG Chairman, and to be approved by H.E. the Governor.
c) The members of the CORWG include representatives from all regulated entities by the Central Bank of Kuwait including Kuwaiti Banks, Foreign Banks, Finance Companies, Exchange Companies, E-Payment of Funds Companies, Credit Information Companies and Open Banking Service Providers.
d) The permanent members of the CORWG include representatives from all Kuwaiti Banks, Foreign Banks operating in Kuwait, Credit Information Companies, and e-Payment Services Operators (EPSOs).
e) CORWG members shall have the right to provide comments and feedback, while the final approval and decision shall be made by the Chairman.
f) Each Regulated Entity shall appoint primary and backup representatives and shall ensure that participation is continuously maintained by nominating replacements in timely manner whenever changes occur.
g) The primary representatives shall hold positions with responsibility of cyber, operational resilience and third-party risk within their respective entity, who have active involvement in strategic initiatives and budgetary matters related to cybersecurity, operational resilience and third-party risk.
h) The backup representatives shall be senior individuals with expertise in cyber, operational resilience and third-party risk, capable of supporting the primary representative. The backup representatives will attend CORWG meetings when the primary representative is unavailable within the respective domain expertise.
i) The nomination of both the primary and backup representatives including change of representatives to the CORWG shall be made by the respective Regulated Entity through an official communication to the CORWG Chairman through CBK formal designated communication channels.
j) Acceptance of nominated Regulated Entities' representatives shall be subject to approval of CORWG Chairman.
k) CORWG Secretariat is not a member of the CORWG.
l) CORWG members are required to abide by the Code of Conduct.

5. Roles and Responsibilities

5.1 CORWG Chairman

The CORWG Chairman is responsible for providing leadership and ensuring effective operation of the CORWG. The Chairman shall:

a) Ensure that the CORWG functions properly and in accordance with its TOR;
b) Facilitate active and inclusive participation of all members during meetings;
c) Lead structured discussions on all relevant topics aligned with the objectives of the CORWG related to cyber risks, resilience, regulation, and sector-wide initiatives;
d) Ensure that effective decisions are made, documented, and implemented as appropriate;
e) Approve meeting agendas and key outputs, including minutes of meetings, CORWG recommendations, and related documentation;
f) Provide final approval on CORWG decisions in alignment to the objectives of the CORWG;
g) Initiate and oversee the execution of necessary activities to achieve CORWG objectives;
h) Appoint representatives from CBK Information Security Team to support the operational and administrative functions of the group.

5.2 CORWG Deputy Chairman

The CORWG Deputy Chairman shall support the Chairman in fulfilling the objectives of the CORWG and ensure the continuity in the group's functioning. The Deputy Chairman responsibilities include:

a) Supporting the Chairman in ensuring the effective operation of the CORWG in line with the TOR;
b) Facilitating meetings and discussions as delegated by the Chairman, ensuring active participation by all members;
c) Leading CORWG meetings during the Chairman's absence;
d) Contributing to the review of CORWG outputs and proposed recommendations; and
e) Coordinating with CBK representatives and CORWG members to support implementation and agreed actions.

5.3 CORWG Secretariat

The responsibilities of the Secretariat include:

a) Organizing CORWG meetings, including scheduling, agenda preparation, distribution of materials, and meeting invitations;
b) Documenting and maintaining accurate records of meetings, including attendance, meeting minutes, decisions, and action items;
c) Coordinating the circulation of consultation materials and consolidation of feedback from CORWG members;
d) Supporting the engagement and coordination with non-member organizations and external stakeholders, as directed by the Chairman;
e) Monitoring the progress of action items and decisions to ensure timely implementation and follow-up.

5.4 Member Organizations

Member organizations are responsible for actively supporting the objectives of the CORWG and contributing to the collective efforts to strengthen cyber and operational resilience across the sector. The responsibilities of Member Organizations' representatives include:

a) Committing the necessary resources, time, and subject matter expertise in order to serve the CORWG objectives and activities;
b) Actively participating in CORWG meetings and agenda items, consultations, and initiatives throughout the duration of their membership;
c) Sharing relevant information, such as cyber incidents, escalations, early warnings, sector-specific studies, where appropriate, to support CORWG initiatives and decision-making;
d) Raising cyber and operational resilience related issues and proposing solutions to secure critical assets, and supporting the effective response to cyber incidents and the timely recovery of operations to improve the overall resilience of the sector;
e) Contributing to CORWG-led efforts, such as awareness campaigns, capacity-building initiatives, sector-wide simulation exercises and other relevant activities;
f) Ensuring internal coordination and communication to reflect their entities' position in CORWG discussions and to disseminate CORWG output and expectations internally within their entities; and
g) Adhering to the CORWG Code of Conduct and maintaining confidentiality of all non-public information and materials shared within the Working Group.

6. Code of Conduct

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

6.1 Conduct

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

6.2 Confidentiality

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

6.3 Conflicts of Interest

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

6.4 Attendance

The representatives shall attend all meetings and provide in advance notice (one business day) in case of absence; exceptions will be applied for emergency meetings. Members shall be prepared for the meetings in accordance with the agenda and shall 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 CORWG.

6.5 Invitees

Invitees could be other representatives from the CBK team, Government entities, or subject matter experts (SMEs) from external organizations who are invited to provide an independent input based on their experience and expertise on the subjects under discussion during the meeting.

In addition, Regulated Entities that are not permanent members of CORWG may be invited to attend meetings or engage in certain activities or simulations, at the discretion of the Chairman, where an agenda item or more is directly relevant to their business.

Invitees are responsible to abide by CORWG's Code of Conduct and are required to keep all meeting engagements and discussions confidential, where they shall not attend a meeting unless they adhere to the CORWG code of conduct. Invitees are only allowed to join the CORWG sessions only with prior approval from the CORWG Chairman and strictly for the time slot and agenda items for which they have been invited.

7. Frequency of Meetings

a) The CORWG meetings will be held at least once every quarter or whenever deemed necessary by the CORWG Chairman. Member organizations that require additional CORWG meetings shall submit a request through email to the CORWG Chairman.
b) Decision to hold additional CORWG meeting or to cancel or defer a meeting within the scheduled cycle will be held at the discretion of the CORWG Chairman.

8. Communication Protocol

All communications related to the CORWG shall be coordinated and centralized by CBK. Official communication with the members – including -but not limited to- meeting invitations, agenda, meeting minutes, consultations materials, and follow-ups – shall be managed by CBK representatives serving as the CORWG secretariat. Communication shall be made through formal CBK secure channels (e.g., email, official memoranda/letters, designated platforms). Member organizations' representatives are responsible for appropriate internal dissemination of CORWG-related information and decisions within their respective entities.

The following communication principles apply for CORWG meeting documentations:

a) **Meeting Agenda** - The meeting agenda will be distributed to the members at least two business days prior to the CORWG meeting, so that members can prepare accordingly. Exceptions will be made for emergency meetings at the discretion of the CORWG Chairman. Member organizations can request to include certain discussions by contacting the CORWG Secretariat.
b) **Meeting Minutes** - Meeting minutes serve as an official record of the meetings of the CORWG. The meeting minutes shall be recorded by the CORWG Secretariat and distributed to members after the CORWG meeting. Members will be requested to provide any comment or feedback within a period of time defined within the CBK communication. If no comments are received within this period, the minutes shall be considered final. If comments are received, a revised version shall be shared, if necessary.

c) **Follow-up and Reporting** - The CORWG primarily works on the basis of an agenda, discussions, presentations, and minutes. Some of the action items may lead to additional initiatives or activities that are eventually executed separately, and are reported back as updates in subsequent presentations to the CORWG.

All communications are subject to the Code of Conduct, and confidentiality shall be maintained at all times by members and participants.

9. Document Management and Version Control

To ensure consistency, traceability, and secure dissemination of all CORF documents, a centralized and controlled approach to document management shall be adopted. This includes the creation, review, circulation, storage, and archival of all relevant documents, in accordance with CBK related governance instructions and defined protocols.

9.1 Centralized Repository

All documents associated with the CORF, including the framework documents; Framework, Toolkit, and Baselines, in addition to all associated templates, reference materials, circulars, CORWG Minutes of Meetings (MoMs), and official communications, shall be maintained on a centralized documentation platform designated by CBK. This platform shall serve as the official repository and single source of truth of all CORF relevant documentation.

Access to this centralized documentation platform shall be granted and managed on a role-based basis, ensuring that:

- All CORWG members shall be granted view access to all published CORF documents, and the permission to provide comments only when and where explicitly authorized by CBK.
- Access to documents intended for specific Regulated Entities shall be restricted to the authorized representatives of the respective targeted entities only.
- When documents are shared for consultation purposes, the right to provide comments and feedback shall be granted to the CORWG members and any other participants explicitly nominated by the relevant Regulated Entities, within a defined time period as specified by CBK.
- The administration of the platform and the management of user access shall be under CBK's management.

9.2 Version Control

All CORF documents shall follow a structured version control process:

- Each document must clearly indicate its version number, date of issue, author(s), reviewer(s), approver(s), and a summary of changes.
- Major revisions (e.g., v1.0 to v2.0) must be formally reviewed and approved by the CORWG and documented in the MoM.
- Minor updates (e.g., v1.1 to v1.2) may be carried out by CBK, but must include a brief concise description of changes and be logged in the relevant version history section in the documentation platform.

9.3 Documents Retention and Archival

- Superseded or obsolete versions of documents shall be archived in a designated section of the platform and clearly marked as "Superseded/Obsolete" to prevent unintentional reference or use.

- Documents that are shared for review purposes must be clearly marked as “Draft” indicating that they are not to be treated as final or binding.
- Documents shall be retained on the platform for as long as deemed necessary by CBK, in accordance with its policies and regulatory and legal considerations.

10.Review and Update

The CORWG Terms of Reference shall be reviewed and updated as part of the overall review of the Cyber and Operational Resilience Framework (CORF), or earlier if deemed necessary by the CBK. Any reviews or updates should be discussed with the CORWG members and any changes made to the Terms of Reference shall be approved by the CORWG Chairman.

11.Contact Information

All communication from member organization representatives shall be addressed to the CBK representatives via CORWG@cbk.gov.kw

Chapter 3:
Cyber and Operational Resilience Framework Toolkit

DOCUMENT CONTROL

Date	Version	Author	Change Reference	Reviewer/ Approver
03 Dec 2025	1.0	Central Bank of Kuwait	First Release	Central Bank of Kuwait

Table of Contents

1. Introduction

The Cyber and Operational Resilience Framework (CORF) Toolkit is an essential element of the broader CORF suite, designed to operationalize the key components of the framework through providing a structured practical guidance and standardized instruments for the Regulated Entities under the CORF. While the rest of CORF documents establishes the "what", the Toolkit clarifies the "how", bridging the gap between high-level expectations and the on-ground implementation, translating these into consistent and actionable measure.

More than just a reference, the Toolkit is a practical enabler, equipping Entities with standardized instruments and the tools necessary to interpret and apply the CORF requirements with precision. This would ensure uniform understanding and implementation across the sector.

Through its guidance materials and integrated templates, the Toolkit supports integrity and consistency of assessments, enhances comparability across the sector, and promotes supervisory engagement.

2. Purpose

The main purpose of the Toolkit is to provide guidance for Regulated Entities and assessors in a clear and structured manner. Specifically:

- Supporting the development of a Statement of Applicability (SoA), clearly defining applicable controls and justification for exclusions;
- Enabling accurate and uniform implementation of the assessment criteria;
- Providing structured guidance for completing the inherent risk profiling, to enable forward-looking risk visibility and facilitate supervisory tiering;
- Defining cyber resilience workforce framework and its application; and
- Outlining the obligations of the Regulated Entities under the CORF.

3. Toolkit Structure

The CORF Toolkit comprises of four (4) main components:

- **Statement of Applicability (SoA)** – Provides instructions and templates for completing and submitting the SoA, as a mandatory deliverable under the CORF;
- **Assessment Criteria Guidelines** – Provides comprehensive guidance on the dual-layered assessment approach, covering both compliance and maturity. It includes clear instructions, scoring logic, and maturity levels descriptions, enabling both Regulated Entities and assessors to evaluate cybersecurity and resilience posture in a structured and consistent manner;
- **Inherent Risk Profiling** – This component supports the categorization of the Regulated Entities into the appropriate supervisory tier based on the inherent risk. It includes structured set of assessment criteria grouped by defined tiering dimensions, input formatting guidance, and instructions for accurate and complete submissions; and
- **Cyber Resilience Workforce Framework** – This outlines the required cybersecurity functions, roles, and considerations to establish a comprehensive sector-wide approach for developing and sustaining cybersecurity talent across the sector.

4. Statement of Applicability

The Statement of Applicability (SoA) is a mandatory submission required from all Regulated Entities under the supervision and oversight of the CBK. It serves as a formal declaration of which domains and sub-domains within the Cyber and Operational Resilience Framework (CORF) are applicable to the entities, based on their licensed activities, business model, and services provided.

The main purpose of the SoA is to ensure that all types of assessments (i.e., self-assessments and independent assessments) conducted against the CORF are accurate, risk-based, proportionate, and relevant to the entity's business profile.

4.1 Applicability and Submission Requirements

The SoA must be submitted by all entities regulated by the CBK. This includes:

- Kuwaiti Banks;
- Foreign Banks operating in the State of Kuwait;
- Exchange Companies;
- Finance Companies;
- E-Payment of Funds Companies;
- Credit Information Companies; and
- Open Banking Service Providers.

The SoA shall be prepared and submitted prior to being assessed against the CORF, whether such assessment is conducted by the CBK, designated third-party assessor or as part of the self-assessment process to establish the initial scope of the Framework's applicability.

The SoA shall be submitted in the outlined prescribed format (Refer to Section 8.1) and is subject to CBK's formal review and approval. It will serve as the official reference for determining the applicable scope during both self-assessments and independent assessments.

4.2 Importance of SoA

Submitting a complete, accurate, and well-justified SoA plays a central role and is critical to the integrity and effectiveness of the assessment process, as it:

- Clearly defines the applicable scope based on the entity's actual business profile;
- Ensures transparency and accountability in the declaration of exclusions;
- Supports consistency and fairness across various types of entities within the sector; and
- Enables CBK to have a targeted oversight and reduces unnecessary compliance burden.

Submission of an incomplete, inaccurate, or unjustified SoA, may result in rejection, assessment delays, regulatory observations, or findings of non-compliance. Therefore, regulated entities are expected to exercise due diligence and engage all relevant stakeholders internally to ensure that the SoA reflects their operational environment in an accurate way.

4.3 Structure and Content

The SoA must include the following components:

- A complete list of all CORF domains and sub-domains;
- A clearly stated "Applicability Status" per each item (i.e., Applicable or Not Applicable); and
- A clear detailed justification for each domain and/or sub-domain marked as "Not Applicable".

The SoA shall be limited to the applicability declarations at the CORF domain and sub-domain level only. Individual controls shall not be excluded via the SoA on technical or implementation-specific factors (e.g.,

non-use of Cloud services, APIs, mobile platforms). Such considerations shall be addressed and documented during the assessment process, not as part of the SoA.

4.4 Criteria for Exclusion

Exclusion of a CORF domain or sub-domain may be permitted only where it is demonstrably not relevant to the entity's operations and activities. Acceptable ground include:

- The entity does not offer relevant business services or functions;
- The function is implemented centrally at the group level, with proper oversight and assurance mechanisms in place; or
- Legal and regulatory constraints prevent implementation at the local level.

CBK reserves the right to reject exclusions that are insufficiently substantiated or that are relevant to critical sector-wide requirements.

4.5 Review and Update

The SoA must be reviewed and updated on regular basis, to remain accurate and reflective of the Entity's current operations. At a minimum, the SoA shall be:

- Reviewed and revalidated at least annually; and
- Updated following any material change that might affect the applicability of any CORF domain or sub-domain, including -but not limited to- changes in licensed activities, provided services, legal or regulatory obligations, organizational structure, or group-level arrangements.

If any change occurs outside the scheduled assessment cycle, an updated SoA must be submitted to CBK in timely manner.

4.6 SoA Template

All Regulated Entities shall use the official SoA template provided in the **"Templates"** section of this document when preparing and submitting their SoA. The template must be used without any modification.

5. Assessment Criteria Guidelines

The assessment criteria define the structured methodology to assess the cybersecurity and resilience posture of Regulated Entities subject to the CORF. This methodology is designed to deliver a dual-layered, consistent, and more objective approach that enables CBK to evaluate both the implementation of the required baseline controls and the maturity of the institutionalized cybersecurity and resilience practices.

This section provides a clear guidance to the Regulated Entities and assessors on how to assess compliance with the CORF Baselines and determine maturity levels across sub-domains and domains.

5.1 Assessment Objectives

The CORF assessment methodology has three key objectives:

- Provide standardized and verifiable criteria to reduce subjective interpretation;
- Enable benchmarking across Entities and domains; and
- Reflect incremental maturity and encourage continuous improvement in cybersecurity and resilience capabilities.

5.2 Assessment Structure

The assessment structure consists of two complementary layers; compliance assessment and maturity assessment, as illustrated in the following sub-sections.

5.2.1 Compliance Assessment

Each control in the Cyber and Operational Resilience Baselines, Operational Resilience Baselines, TPRM Baselines are assessed for compliance, where this is done through two essential tests:

- **Test of Design** – Confirms that the control is appropriately designed, documented, and contextualized to the Entity's operations and risk environment.
- **Test of Effectiveness** – Verifies that the control is functioning as intended, supported by evidence such as system configurations, logs, monitoring outputs, or reports.

Accordingly, every control is evaluated and rated on a binary basis:

- **Compliant** – The control is fully implemented and verifiably effective.
- **Non-Compliant** – The control is not in place, ineffective, or lacks supporting evidence.
- **Not Applicable** – Control is irrelevant to the Entity's operations, subject to formal justification and CBK approval.

This binary model ensures objectivity and eliminates subjective or partial interpretations. It also promotes clear accountability and uniformity across assessments. The results of control-level compliance assessments are used to calculate:

- **Sub-Domain Compliance Score** – Percentage of applicable controls marked as "Compliant" within each sub-domain.
- **Domain Compliance Score** – Aggregated compliance percentage based on all sub-domains under the domain.
- **Overall Compliance Score** – Rolled-up average across all domains, offering Entity-specific and sector-wide compliance view.

5.2.2 Maturity Assessment

Each sub-domain is assessed using a standardized five-level maturity model designed to evaluate how well cybersecurity and resilience capabilities are embedded, institutionalized, automated, innovative, and continuously improved. The five levels are:

- **Level 1 – Initial** - Reactive and unstructured cybersecurity approach with informal practices. Lacks formal documentation and consistent implementation.
- **Level 2 – Ad-hoc** - Basic, fragmented, and inconsistent practices with some plans to incorporate best practices and regulatory guidelines. Significant gaps remain in the coverage and implementation of controls.
- **Level 3 – Baseline** - Risk-based and well documented cyber and operational resilience practices and procedures are in place, regularly maintained, performance measured, and implemented in a structured and compliant manner.
- **Level 4 – Advanced** - Strategic and proactive integration of cyber and operational resilience with business goals, supported by automation, visibility, and continuous improvement.
- **Level 5 – Innovative** - Anticipatory and advanced technology-driven (e.g., AI-driven) practices with real-time capabilities that continuously enhance resilience, enable adaptive response, and promote/support sector-wide innovative practices and collaboration.

Maturity ratings shall reflect demonstratable achievement of the attributes defined at each level. A Regulated Entity cannot be assessed at Level 3 – Baseline or higher, unless it has achieved full compliance with all applicable controls within that sub-domain. This ensures maturity assessments are grounded in practice rather than perception.

This model is progressive in nature, meaning that advancement to higher levels requires full and demonstratable achievement of the preceding one, ensuring that improvements are meaningful and sustainable.

To assist Regulated Entities and assessors in determining the appropriate maturity levels, maturity attributes are defined per each sub-domain within the CORF, as detailed in Appendix A of this Toolkit. These attributes describe the expected capabilities and characteristics at each maturity level to form the basis for a standardized assessment, benchmarking, and progression tracking. In general, the attributes at each level are characterized by the following:

Framework-Level Maturity Attributes Definitions				
Level 1 – Initial	**Level 2 – Ad-hoc**	**Level 3 – Baseline**	**Level 4 – Advanced**	**Level 5 – Innovative**
▪ Activities are informal, reactive, and inconsistently applied across the regulated entity. ▪ There is no formal documentation of standards, policies, procedures, or processes. ▪ Decisions are made without	▪ Partial documentation exists, but practices are ad-hoc, not standardized or institutionally adopted. ▪ Controls are partially or inconsistently implemented. ▪ Efforts are siloed, with	▪ Comprehensive documentation of standards, policies, procedures, and processes are formally documented, approved, regularly reviewed, and updated.	▪ Sub-domain processes are centralized and automated. ▪ Real-time monitoring and advanced analytics are in place and integrated to provide enterprise-wide visibility	▪ Sub-domain implementation is anticipatory, intelligence-led, and continuously refined based on real-time risk indicators and threat modelling. ▪ Cutting-edge technologies, including AI and

Framework-Level Maturity Attributes Definitions				
Level 1 – Initial	**Level 2 – Ad-hoc**	**Level 3 – Baseline**	**Level 4 – Advanced**	**Level 5 – Innovative**
awareness or consideration of cyber risks, threats, or organizational context.	limited or no coordination or accountability. ▪ Intent or initial informal plans to align with regulations, industry standards, and best practices are in place, but remain largely unimplemented. ▪ Incident learning and data retention are inconsistent and rarely influence current practices. ▪ Performance metrics are unavailable or unreliable, limiting the ability to monitor and improve baseline controls.	▪ Risk assessments, threat intelligence, and business impacts inform resilience planning and implementation. ▪ Proactive approach to resilience with structured implementation of baseline controls. ▪ Learnings from incidents, testing exercises, and threat trends are integrated into continuous improvement cycles. ▪ Alignment with legal and regulatory requirements, in addition to global industry standards and best practices is maintained and demonstratable. ▪ Performance metrics and dashboards are used to monitor compliance and controls effectiveness on regular basis.	into risks and performance. ▪ Workflows and alerts are streamlined through automation, improving operational efficiency and effectiveness. ▪ Resilience strategy and practices are in line with the wider business goals. ▪ A largely proactive resilience posture is achieved through automation, enabling early detection and response to emerging threats. ▪ Continuous improvement through quantitative understanding of processes. ▪ Processes have been optimized to a level of leading practices, based on insights from continuous process improvement	ML, are fully integrated to enable predictive analysis, automated response, strategic decision support, and enable adaptive responses to changes. ▪ Resilience practices are dynamically aligned with evolving risk tolerances, business needs, and sectoral developments. ▪ Real-time monitoring and AI-powered dashboards are in place to provide management with continuous situational visibility and actionable insights, to enhance decision-making and operational efficiency. ▪ The regulated entity contributes to sector-wide innovation, information

Framework-Level Maturity Attributes Definitions				
Level 1 – Initial	**Level 2 – Ad-hoc**	**Level 3 – Baseline**	**Level 4 – Advanced**	**Level 5 – Innovative**
			and maturity modeling.	sharing and resilience.

To reflect the overall posture of each domain within the CORF Baselines document, domain maturity level is calculated by averaging the maturity levels of all associated sub-domains under that specific domain. Then, the overall cyber maturity level of the Regulated Entity is determined by averaging the maturity levels across all six domains defined in the CORF Baselines document.

This overall cyber maturity level serves as a high-level indicator of the Regulated Entity's cyber and operational resilience posture and supports sectoral benchmarking and risk analysis, supervisory tiering, and regulatory prioritization, in addition to informing the development of targeted capacity-building programs.

5.3 Reporting Requirements

Regulated Entities shall submit assessment results to CBK in the format prescribed in the "Templates" section in this Toolkit. This includes:

- **Compliance Reporting** – Entities shall report the compliance status for each individual control, along with the aggregated compliance percentages at sub-domain, domain, and overall levels. For the controls that are assessed as "Not Applicable", these shall be formally justified in the report and approved by CBK.
- **Maturity Reporting** – For each sub-domain, Regulated Entities shall report the assessed maturity level, accompanied by the rationale and supporting commentary. Domain and overall maturity levels shall be also calculated and presented in the report.

All Regulated Entities shall complete and submit assessment outcomes according to the following frequencies:

- **Self- Assessment** - This assessment shall be conducted and submitted on an annual basis.
- **Third-Party Assessment** – Each Regulated Entity shall engage an independent third-party assessor on annual basis and/or as directed by CBK to conduct an assessment against the CORF and report the results to the CBK. The assessor shall be a CBK-approved assessor.

Furthermore, CBK will conduct CORF assessments for the Regulated Entities based on the frequency corresponding to the supervisory tier in which the Entity is categorized, as defined in the Cyber and Operational Resilience Framework.

6. Inherent Risk Profiling

Inherent risk profiling is a foundational component of the CORF, enabling CBK to assess the level of cyber and information security risk that each Regulated Entity is inherently exposed to, prior to considering the mitigation effectiveness of any existing cybersecurity or resilience controls.

This exercise provides a forward-looking view of an Entity's systemic importance, exposure surface, and digital complexity and interconnectedness, based on its operational scale, service offerings, technology environment, and interdependencies.

The primary objective of this profiling is to form the basis for a proportionate and risk-informed supervisory tiering. By objectively evaluating each Entity's characteristics, CBK is able to categorize Regulated Entities into one of the three supervisory tiers: High-Impact, Medium-Impact, or Low-Impact Entities. This categorization determines the level of oversight intensity, assessment frequency, and other regulatory expectations under the CORF.

At the sectoral level, inherent risk profiling also provides CBK with insights and comprehensive view of risk distribution, systemic exposure across the sector, technology adoption, interdependencies, and concentration points of critical services. This visibility informs and supports regulatory planning and prioritization, targeted capacity-building, resilience policy formulation, and coordinated incident response planning. Thereby, enhancing the overall national cyber resilience.

This section provides guidance for Regulated Entities to complete the inherent risk profiling exercise and explains its alignment with the tiering model defined in the Framework document.

6.1 Scope and Applicability

The inherent risk profiling applies to and is mandatory for all Regulated Entities subject to the CORF, where:

- Regulated Entities shall submit it as part of the initial onboarding under this CORF and updated annually, or upon significant changes to operational, technological, or organizational landscape.
- Responses and inputs shall be provided completely, truthfully, and accurately, reflecting actual and up-to-date status without any misrepresentation, omission, or falsification of information.
- Selected criteria will be populated or validated by CBK Supervision Department, particularly those that are regulatory and supervisory in nature.
- CBK may request clarifications or supporting evidence to validate any input provided.

6.2 Tiering Dimensions

The inherent risk profiling is structured around eleven (11) tiering dimensions, as defined in Section 10 of the Framework document. Each dimension reflects a specific attribute of an Entity's inherent exposure or systemic role:

- **Total Number of Assets** – Reflects the financial scale of the entity and its potential impact on the overall stability of the sector.
- **Market Share** – Indicates the entity's dominance or influence within the respective financial segment (e.g., deposits, loans, digital payments).
- **Branch Network and Channels** – Evaluates the geographic spread and delivery mechanisms (e.g., physical branches, neobanks, mobile applications, ATMs/ITMs) that contribute to the entity's exposure and operational footprint.

- **Customer Base** – Considers the size and diversity of the customer population served, and the potential impact of service disruption.
- **Nature and Breadth of Services** – Assesses whether the entity provides retail banking, corporate banking, investment, financing, or payment services, including digital and cross-border offerings.
- **Infrastructure Role** – Includes designation as an FMI, such as operators of payment gateways, credit information networks, or other essential platforms.
- **Technological Complexity** – Covers the extent of emerging and advanced technologies usage, such as Cloud adoption, use of APIs, AI/ML, and integration with digital platforms.
- **Outsourcing and Third-party Dependencies** – Evaluates the level of interconnectivity with third-parties and reliance on outsourcing.
- **Cyber Risk Exposure and Threat Landscape** – Involves the attack surface introduced by digital transformation, legacy systems, or public-facing systems/platforms.
- **Regulatory and Supervisory History** – Considers CBK's previous audit findings, cyber incidents that revealed material weaknesses in cybersecurity and resilience posture, and responsiveness to regulatory requirements.
- **Cyber Resilience Workforce –** Takes into consideration the number of directly attributed personnel working on cybersecurity initiatives to ensure proportionate coverage given potential exposure.

The dimensions have been defined to capture true scale, exposure, and systemic relevance of each Regulated Entity in a way that is structured, consistent, and aligned with supervisory priorities. Collectively, these dimensions provide a comprehensive view through which CBK can determine the inherent risk posture pf each Regulated Entity.

6.3 Structure of the Template

The inherent risk profiling template is comprised of (68) structured set of assessment criteria, covering both quantitative and qualitative indicators, each mapped to one of the eleven (11) tiering dimensions. These assessment criteria are designed to ensure consistent, accurate, and comparable responses to extract factual inputs relevant to:

- Organizational scale and customer footprint;
- Market participation, products and services offerings and their complexity;
- Technology landscape and digitization;
- Interdependencies with third-parties;
- Infrastructure role and systemic functions;
- Exposure to cyber threats and disruptions; and
- Cyber resilience workforce size and capability levels.

Each row in the template includes the following fields:

- Tiering Dimension – The inherent risk category to which the assessment criteria relates;
- Assessment Criteria – A clearly defined questions or data point used to evaluate a specific attribute or aspect of the Regulated Entity's exposure;
- Input Guidance – Formatting instructions to ensure consistency of input (e.g., expected unit of measurement, data type); and

- Input Field – The required responses, structured and formatted in a way that required clear input, such as:
    - Quantitative value (e.g., numeric value/range, percentage);
    - Binary responses – Yes/No questions with supporting qualifiers; or
    - Pre-defined selections from drop-down or multi-selection lists.

The responses will be used by CBK to assess the inherent risk posture of each Regulated Entity and categorize them into the appropriate supervisory tier using a risk-based model. The profiling outcomes will support sector-level analysis and facilitate focused engagement and thematic assessments.

The full set of assessment criteria, organized and mapped to their corresponding tiering dimensions, is included in the **"Templates"** section of this Toolkit.

6.4 Review and Update

To ensure ongoing accuracy and relevance, inherent risk profiling shall be maintained as a living document, reflecting each Entity's evolving risk environment, where:

- Regulated Entities shall update the inherent risk profile on an annual basis.
- Updates are also required in response to significant changes, such as:
    - Major re-structuring or acquisition;
    - Shifts in outsourcing agreements and third-party dependencies;
    - Launch of new digital channels or services;
    - Adoption of emerging technologies (e.g., Cloud, Artificial Intelligence, Machine Learning, Quantum Computing); and
    - Changes in cyber workforce composition.
- CBK may request interim updates or clarifications at any time, particularly when significant risk shifts are observed, or sector-wide reviews are being conducted.
- The structure and contents of the inherent risk profiling template will be reviewed and enhanced periodically by CBK in line with the regulatory developments, sector feedback, and emerging risks. Such updates will be formally and clearly communicated to the Regulated Entities through CBK designated communication channels.

7. Cyber Workforce Management Framework

7.1 Overview of Cyber Resilience Workforce Framework - Job Categories, Job Roles, Required Skills, and Qualifications

This Cyber Resilience Workforce Framework (CRWF) is designed to establish a comprehensive and structured approach to developing, managing, and sustaining a skilled and resilient cyber resilience workforce. This framework aims to address the growing demand for cybersecurity professionals across the Kuwaiti banking and financial sector by providing clear guidelines and strategies for workforce development, talent management, and continuous improvement.

The CRWF is designed as a Sector Wide initiative to build a strong, coordinated cybersecurity leadership ecosystem within the Kuwaiti banking and financial sector. The program aligns with national security goals and aims to prepare decision-makers with the mindset, skills, and strategic capabilities needed to navigate today's complex cyber threat landscape. The key objectives are:

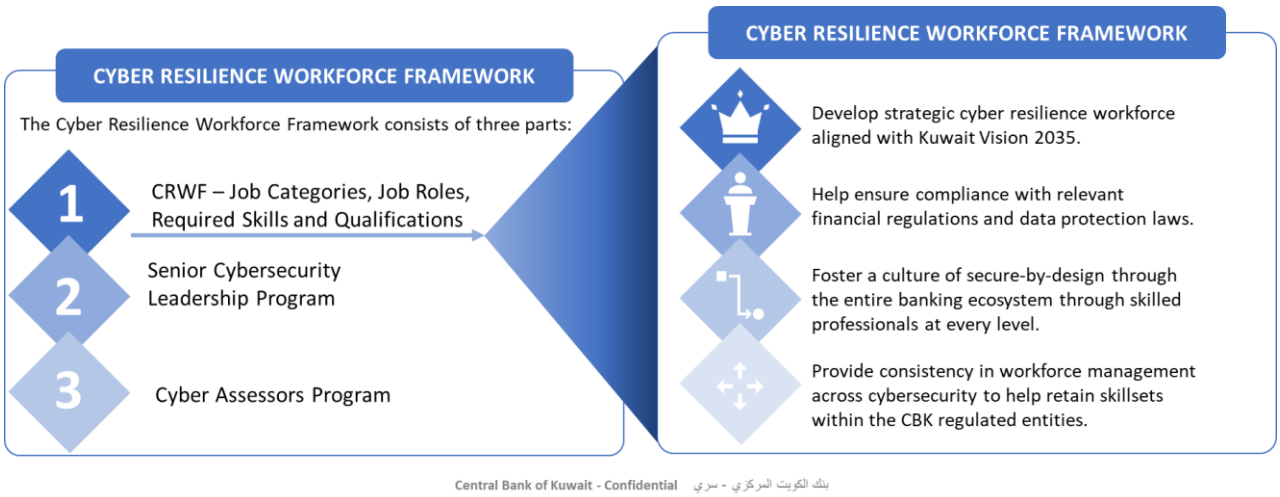


Figure 1. Overview of Cyber Resilience Workforce Framework

These key components collectively form a comprehensive Cyber Resilience Workforce Framework (CRWF) that will help CBK to systematically manage and develop the cybersecurity talent across the banking and financial sector. By clearly defining job categories, roles, proficiency levels, and Knowledge Skills and Abilities (KSA) statements, CBK can ensure that they drive consistency across regulated entities, enabling a stronger internal ecosystem to retain talent, and tackle cybersecurity challenges through to 2030.

The table below presents the Key Pillars for the Workforce Framework:

Cyber Resilience Workforce Framework	Description
JOB CATEGORIES	Job categories are broad classifications that group similar types of work within the cybersecurity field. These categories help to organize the various roles and responsibilities within Kuwaiti FS cyber resilience workforce, making it easier to identify and understand the different areas of expertise required. Job categories are essential for structuring the framework as they provide a high-level view of the different domains within cybersecurity. They help regulated entities to align their workforce needs with specific areas of cybersecurity, ensuring that they have the right mix of skills and expertise to address various challenges.
JOB ROLES	Job roles are specific positions within each job category that define the particular duties and responsibilities of individuals. Each role has a unique set of tasks and functions that contribute to the overall cybersecurity efforts of a regulated entity. Job roles are crucial for detailing the specific functions within each job category. They help the Kuwaiti FS to identify the precise skills and competencies required for each position, facilitating targeted recruitment, training, and development efforts. Clearly defined job roles also aid in career progression and succession planning, thereby supporting their retention in the Kuwaiti banking and financial sector.
PROFICIENCY LEVELS	Controls are standardized and documented, with proactive risk management measures tailored to organizational needs Proficiency levels indicate the degree of expertise and experience required for different job roles. These levels typically range from entry-level to expert, providing a clear pathway for career development within the cybersecurity field. Proficiency levels are important for assessing and developing the capabilities of the cyber resilience workforce. They will help regulated entities to match individuals with appropriate roles based on their skill level and experience, ensuring that tasks are performed effectively and efficiently. Proficiency levels also guide training and professional development initiatives, helping employees to advance their careers.
KNOWLEDGE, SKILLS & ABILITIES	KSA statements describe the specific knowledge, skills, and abilities required for each job role. Knowledge refers to the theoretical understanding of cybersecurity concepts, skills pertain to the practical application of these concepts, and abilities relate to the capacity to perform tasks effectively. KSA statements are fundamental to the framework as they provide detailed criteria for evaluating and developing the cyber resilience workforce. They will assist regulated entities to identify gaps in their employees' competencies and design targeted training programs to address these gaps. KSA statements also support performance evaluations and career development planning, ensuring that employees have the necessary capabilities to succeed in their roles.

7.2 Overview of the CBK Cybersecurity Competency Framework

The **CBK Cybersecurity Competency Framework** should be designed to support the Banking and Financial Sector to build a highly skilled, adaptive, and resilient focused cyber workforce, improving resilience across the regulatory landscape.

	STRATEGIC CONTEXT As cyber threats continue to evolve in complexity and scale, the Central Bank of Kuwait must establish a highly skilled cyber resilience workforce capable of protecting critical assets. The CBK Cybersecurity Competency Framework provides a structured approach to developing, assessing, and maintaining the cybersecurity expertise required to defend against cyber threats, helping to ensure a banking and financial sector resilient to attacks. It serves as the foundational pillar for building a skilled, agile, and mission-ready cyber resilience workforce, designing the required training, and ensuring the CBK remain proactive in addressing current and emerging cyber threats.
	PURPOSE The Framework is designed to: • Define key cybersecurity roles within FS, aligning with operational and strategic needs. • Establish competencies and proficiency levels for personnel across different career stages. • Guide training, professional development and career progression to build a resilient cyber resilience workforce. • Ensure alignment with national and international cybersecurity standards and best practice. • Foster interoperability with partners through standardized skill recognition.
	KEY COMPONENTS The Framework comprises the following elements: 1. **Role-based competency model** - identifies cybersecurity roles and maps them to required competencies. 2. **Core cyber areas and specialisms** – covers essential domains such as risk, security operations, cyber threat intelligence, and identity and access management. 3. **Knowledge, Skills and Abilities descriptors** – defines the core, technical, and complementary qualities required from cyber personnel. 4. **Skill Proficiency Levels** – defines competency tiers to support career progression and growing expertise and multiple diverse skillsets.
	STRATEGIC IMPACT Through implementing the Competency Framework, CBK will: • Strengthen cyber resilience across Regulated Entities. • Enhance Defensive Capabilities through personnel that possess the necessary skills to rapidly detect, respond, and recover from cyber incidents. • Improve talent retention and career progression for cybersecurity professionals in FS. • Enhance collaboration and coordination between FS entities on cybersecurity initiatives. • Ensure operational effectiveness and improved resilience in sector-wide attacks.

7.3 Overview of Kuwaiti Banking and Financial Sector Technical Areas - Job Categories

The Job Categories for the Cyber Resilience Workforce Framework (CRWF) are a derivative of the 7 x NIST NICE Job Categories, the 15 x Specialisms under the UK Cyber Security Council (UKCSC), and the 5 x Career Pathways of the Singapore Computer Society (SCS). The focus is placed on the area's most prevalent in the banking and financial sector, using more traditional Job Categories to align with current Kuwaiti banking and financial sector norms. 9 Job Categories have been initially identified with 49 initial Job Roles. Those areas and the key responsibilities can be found below:

CYBERSECURITY LEADERSHIP	GOVERNANCE, RISK AND COMPLIANCE
Responsible for leading the strategic formulation and execution of the banking and financial sector's Cybersecurity initiatives. Drive the development of advanced cyberspace capabilities and future-oriented cyber resilience workforce strategies. Oversee and mentor high-performing cyber teams to ensure alignment with the sector's Cybersecurity Strategy and national security objectives within the cyber domain.	Responsible for developing and uphold a comprehensive framework of policies, procedures, and controls to ensure the banking and financial sector' cybersecurity practices adhere to applicable laws, regulations, and defense standards, including privacy and legal requirements. Identify, evaluate, and prioritize cybersecurity risks across the sector, and implement robust controls to mitigate those risks effectively, ensuring operational resilience and mission security.
SECURITY ARCHITECTURE	**SECURITY OPERATIONS**
Responsible for spearheading the design and deployment of resilient cybersecurity architectures and systems to safeguard critical defense assets and classified information. Focus on constructing secure network frameworks, systems, and application architectures, implementing robust defensive measures, and ensuring the confidentiality, integrity, and availability of sensitive defense data.	Security Operations emphasizing the protection, monitoring, and analysis of security incidents and intrusions that could compromise defense information systems and networks. Manage the escalation of threats and unauthorized activities, and ensure the continuous optimization, operation, and maintenance of the banking and financial sector's defensive systems and technologies to uphold operational security and integrity.
EMERGING TECHNOLOGY	**CYBERSECURITY THREAT AND INTELLIGENCE**
Emerging Technology in the banking and financial sector involves researching, evaluating, designing, and implementing advanced technologies like AI, ML, Quantum Computing, Quantum-Safe Cryptography, Blockchain, and Cloud Computing to enhance security and efficiency. This specialism is vital for banks to innovate securely, stay competitive, and align with modernization goals such as Kuwait Vision 2035, which aims to transform Kuwait into a financial leader by 2035. Professionals must understand security implications, collaborate	Responsible for collection, analysis, and dissemination of actionable intelligence on cyber adversaries, vulnerabilities, and threats within the cyberspace domain. Facilitate intelligence sharing and coordination across multiple defense forces and organizations within the banking and financial sector, ensuring that relevant stakeholders are informed as needed. Collaborate with security operations teams to anticipate and refine the sector's protective measures, enhancing the capability to detect and respond to emerging threats effectively.

with technical and business teams, and align implementations with national priorities and regulatory requirements. This role demands high technical expertise, foresight, and the ability to navigate rapidly evolving technological landscapes.

VULNERABILITY ASSESSMENT

Responsible for the identification, assessment, and prioritization of vulnerabilities in the banking and financial sector's networks, systems, and applications. Management of these vulnerabilities to reduce risk to banking and financial sector's assets and operations.

IDENTITY AND ACCESS MANAGEMENT

Define and implement a framework of processes and technologies that enable the management of electronic or digital identities and associated permissions to perform functions, access data or administer systems.

DIGITAL FORENSICS AND INCIDENT RESPONSE

Responsible for leading the response and investigation of security incidents within the banking and financial sector, ensuring timely and effective resolution in accordance with established incident response protocols. Manage the full incident response lifecycle, including preparation, detection and analysis, containment, eradication, and recovery from cyber incidents. Conduct digital forensics to uncover and analyze evidence and execute post-incident management to strengthen defenses and refine response strategies.

7.4 Overview of Job Roles and Levels

The CRWF uses 3 levels to articulate the expected Proficiency Level which you might have against your skills, your amount of experience in Cyber and the training you should have carried out. The levels, as described below, are intended to be generic descriptors. More detailed descriptors of each level, tailored to specific technical areas, would be found in the detailed descriptors in a fully developed version of the CRWF.

CYBERSECURITY LEADERSHIP	GOVERNANCE, RISK AND COMPLIANCE
• Chief Information Security Officer (CISO) • Cyber Workforce Management • Cybersecurity Policy & Planning Officer • Director of Information & Cyber Security • Head of Cyber Security • Business Continuity and Disaster Recovery Manager • Training and Awareness Manager	• Cybersecurity Governance Officer • Cybersecurity Risk Officer • Cybersecurity Compliance Officer • Security Controls Assessor • Security Auditor • Third-Party Risk Manager • Data Privacy Officer • Cyber Fraud Officer
SECURITY ARCHITECTURE	**SECURITY OPERATIONS**
• Chief Security Architect • Security Architect • Cloud Architect • Application Security Architect • Emerging Technology / AI Architect • Systems Security Engineer • Cloud Infrastructure Security Engineer • Applications Security Engineer	• Security Operations Centre (SOC) Analyst • Security Operations Centre (SOC) Manager • Security Information and Event Management Engineer • Network Security Engineer
EMERGING TECHNOLOGY	**CYBERSECURITY THREAT AND INTELLIGENCE**
• Head of Emerging Technology • AI Governance & Risk Manager • Emerging Technology / Artificial Intelligence Security Engineer • Blockchain Security Engineer • Quantum Security Engineer • Quantum-safe Cryptography Engineer	• Cyber Threat Intelligence Manager • Cyber Threat Intelligence Analyst • Cyber Threat Hunter • Cyber Risk Modeler
VULNERABILITY ASSESSMENT	**DIGITAL FORENSICS AND INCIDENT RESPONSE**
• Vulnerability Management Manger • Vulnerability Assessment Analyst • Penetration Tester • Vulnerability and Patch Management Specialist	• Cybersecurity Incident Responder • Cybersecurity Incident Coordinator • Digital Forensics and Incident Response Manager • Digital Forensics Specialist
IDENTITY AND ACCESS MANAGEMENT	**FUTURE DEVELOPMENT**
• IAM Manager • IAM Analyst / Engineer • Privileged Access Management Eng. • Authentication Engineer • Customer Identity Specialist	To ascertain the exact needs of the Kuwaiti banking and financial sector, a deep study over 3+months would be required. This would provide detailed Job Roles with specific Knowledge, Skills, and Abilities statements.

7.4.1 Job Levels

a. Level 1: Specialist

Individuals at this level have a basic understanding of cybersecurity and can describe the process and concepts related to their competence. They can apply basic skills under supervision and undertake low-level output delivery.

They may have completed introductory training or have some prior experience in a related field.

b. **Level 2: Senior Specialist**

Individuals at this level have a solid understanding of cybersecurity and can apply specialist knowledge and skills to a variety of tasks, some of which are complex. They can work independently and are able to provide support and guidance to junior Cyber operators in their Area. They may have completed intermediate-level training or have several years of experience in a related field.

c. **Level 3: Expert**

Individuals at this level have shown an in-depth expertise in a wide variety of complex tasks. They have expertise in the delivery of operational outputs. They can provide support, guidance, and mentorship to individuals in their Area and have experience with leading teams.

They have completed specialized training and have many years of experience in their field.

7.4.2 Career Cards

1. CYBERSECURITY LEADERSHIP

Cybersecurity Leadership is a senior role within the organization responsible for managing cybersecurity resources, staff, and policies at an enterprise level. This leadership ensures that cybersecurity efforts are applied efficiently and effectively to protect the organization's systems, services, and information, aligning with business objectives and regulatory requirements. Leaders in this specialism establish and operate the cybersecurity strategy, working closely with other senior managers and serving as the primary point of contact on cybersecurity issues across the organization and externally. Key responsibilities include setting and managing policies, ensuring compliance, managing staff and resources, contributing to organizational strategy, and advising senior management on cybersecurity effectiveness. In CBK banking and financial sector, this would specifically involve overseeing the security posture protecting assets, customer data, and critical infrastructure, ensuring compliance with relevant regulations and data protection laws. This role requires a high-level understanding of risk management and governance.

Cybersecurity Leadership
Level 1: Specialist
May function as a team leader or senior professional responsible for one or several cybersecurity functions within a smaller organization or department. Focuses on ensuring adherence to established policies and procedures, contributing to operational planning, and managing specific security functions or resources under direction.
Knowledge, Skills, and Abilities
Requires knowledge of core cybersecurity domains and established security policies, standards, and procedures. Skills include working within organizational policies and constraints, encouraging colleagues, and contributing to shared objectives. Abilities include effectively managing resources allocated to their function and monitoring performance. In CBK banking and financial sector, this would involve managing security operations or specific functions protecting assets and data.

Cybersecurity Leadership
Level 2: Senior Specialist
Manages a team or department of cybersecurity professionals, overseeing resource allocation, project delivery, and operational effectiveness. Identifies requirements for and monitors the production and updating of policies, sets and monitors compliance with operational standards, and works with managers in other teams to ensure effective cybersecurity across the organization. Engages with heads of business departments to demonstrate cyber risks and recommend changes.
Knowledge, Skills, and Abilities
Needs a solid understanding of risk management methodologies and legal/regulatory requirements. Skills involve directing, developing, or maintaining organizational policies and standards, overseeing compliance monitoring, engaging with business departments on risks, and managing teams. Abilities include interpreting requirements, evaluating the impact of actions, and influencing others. In CBK banking and financial sector, this includes understanding and applying regulations and data protection laws (like PCI-DSS or GDPR) and managing risks specific to systems and data.

Cybersecurity Leadership
Level 3: Expert
Holds a Chief Officer role, such as Chief Information Security Officer (CISO). Directs and operates the overall enterprise cybersecurity strategy, contributes to the organization's high-level strategy, and advises senior management on the effectiveness of the strategy. Is the primary point of contact for key stakeholders internally and externally, manages governance and risk management professionals, and leads cultural change on cybersecurity at an organizational level.
Knowledge, Skills, and Abilities
Requires deep knowledge across areas including Risk Management & Governance, Law & Regulation, and Security Operations & Incident Management. Core abilities include directing and overseeing enterprise security governance, setting and driving information security strategy, leading behavioral and cultural change, engaging with regulatory authorities. In CBK banking and financial sector, this means setting strategy to protect critical infrastructure and customer assets, ensuring compliance with a complex regulatory environment, and communicating risks effectively to the highest levels of the organization.

SUGGESTED QUALIFICATIONS

While the sources point to separate certification frameworks, relevant qualifications for Cybersecurity Leadership roles would typically cover Risk Management & Governance, Legal & Regulation, and Management/Strategy. Senior and Expert levels would benefit from qualifications demonstrating leadership and enterprise-level strategic capabilities. Examples might include CISSP, CISM, CRISC, or relevant business/management certifications.

2. GOVERNANCE, RISK, AND COMPLIANCE

Governance, Risk and Compliance (GRC) involves monitoring compliance with agreed cybersecurity policies and assessing and managing relevant risks. This specialism is crucial for protecting an organization's information systems and data from internal and external threats. Key activities include drafting policies, carrying out risk assessments, verifying compliance, and maintaining risk registers. Audit and Assurance, a component of GRC, focuses on verifying that specified security controls are implemented and effective, often acting as a last line of defense against errors in implementation or maintenance. Data Protection and Privacy, another key aspect, ensures compliance with legal and regulatory standards concerning personal data. Professionals in this area must understand the value of organizational assets, collaborate with various

teams, and present findings clearly to both technical and general management. In CBK banking and financial sector, GRC ensures the security posture aligns with stringent regulations, manages risks associated with financial data and transactions, and audits the controls protecting critical banking infrastructure.

Governance, Risk and Compliance (GRC)
Level 1: Specialist
Focuses on practical risk management duties such as drafting policies, carrying out specific risk assessments, and verifying compliance with policies. May assess the correctness of risk assessments, use auditing tools, review compliance with legal/regulatory requirements, and write formal reports. May also provide support in designing data privacy requirements and assisting in the notification of data breaches.
Knowledge, Skills, and Abilities
Requires understanding of Risk Management & Governance and Law & Regulations. Skills include assessing risk assessments, using auditing tools, reviewing compliance, writing formal reports, and implementing policies. Abilities include attention to detail, methodical approach, and clear communication. In CBK banking and financial sector, this means understanding and applying specific regulations (like PCI-DSS) to risk assessments and compliance reviews, and handling customer data protection requests.

Governance, Risk and Compliance (GRC)
Level 2: Senior Specialist
Has at least three years of cybersecurity experience. Oversees compliance monitoring and reporting to senior management. Sets up and maintains arrangements for managing cybersecurity risk, including organizational structures and lines of authority. May manage GRC professionals. Takes a leading role in information security and data privacy risk compliance audits and promotes data protection awareness. May manage a cryptographic programme (relevant to securing sensitive data).
Knowledge, Skills, and Abilities
Needs deeper knowledge in Risk Management & Governance and Law & Regulations. Skills include implementing and managing specific legislation like the Data Protection Act, managing risk management arrangements, and leading compliance audits. Abilities include reasoned judgement, analytical skills, and sensitive communication when challenging ideas or engaging stakeholders. In CBK banking and financial sector, this involves interpreting complex sector regulations and integrating them with operational requirements, assessing risks to financial data systems, and ensuring privacy is maintained.

Governance, Risk and Compliance (GRC)
Level 3: Expert
Contributes to an organization's high-level risk strategy and defines its risk appetite. Holds titles like Head of Security, Governance Risk & Compliance, Head of Cyber Risk and Assurance, or potentially Head of Data Protection and Privacy. Approves policies and procedures. Assesses and reports on the effectiveness of risk management standards. This may involve tracking the developments of quantum-based cryptography and developing the strategic roadmap.
Knowledge, Skills, and Abilities
Requires comprehensive knowledge of Risk Management & Governance, Law & Regulations, and Human Factors. Skills involve setting risk management arrangements, contributing to high-level risk strategy, and demonstrating leadership in governance. Abilities include taking account of multiple complex factors, presenting objective reasons for decisions, and influencing stakeholders. In CBK banking and financial sector, this means defining the organization's risk appetite for cybersecurity impacting financial operations, ensuring regulatory compliance at the highest level, and embedding a security culture.

SUGGESTED QUALIFICATIONS

Relevant qualifications cover Risk Management & Governance, Law & Regulations, and Audit principles. Examples mentioned include applying standards like COBIT 5 or ISO 27001. Qualifications at higher levels would demonstrate expertise in security management systems, enterprise governance, and interpreting legal frameworks. Certifications like CISA, CISSP, CISM, CRISC, and CIPP/E would be relevant.

3. SECURITY ARCHITECTURE

Security Architecture is the design of IT systems to meet specific security requirements while balancing functional needs. This specialism focuses on solving complex security problems by selecting and integrating technological components and structures, and these design decisions fundamentally determine the security posture of an organization's information systems and networks. Architects create technical requirements and specifications, estimate costs, and ensure systems are developed and implemented securely according to design and industry standards. They provide expert security advice to developers and operators. The role is highly technical and requires collaboration with other specialists, including external suppliers. In CBK banking and financial sector, Secure System Architecture involves designing secure systems for handling sensitive financial data, processing transactions, and protecting critical banking infrastructure, ensuring compliance with relevant security standards and principles like Zero Trust, Security-by-Design, and Privacy-by-Design.

Security Architecture
Level 1: Specialist
Works on interpreting requirements, designing secure software development and delivery systems, creating technical requirements/specifications for systems/subsystems, and providing expert software security advice on design, coding, and testing. Ensures systems are developed and implemented securely according to agreed designs and standards.
Knowledge, Skills, and Abilities
Requires good understanding of Secure Software Lifecycle and relevant security requirements. Skills include interpreting requirements, technical design, providing expert advice, and applying standards. Abilities include logical and methodical thinking, analyzing complex problems, and describing designs clearly. In CBK banking and financial sector, this involves designing secure coding practices and system components for financial applications, considering data protection regulations.

Security Architecture
Level 2: Senior Specialist
Takes a leading role in designing secure systems. May design secure systems to run on cloud platforms. Applies threat intelligence input to design decisions and uses risk assessment results to design management measures. Reviews installations of new network devices. Research potential threats and emerging technologies. Produces system architecture specifications and designs.
Knowledge, Skills, and Abilities
Needs solid understanding of Operating Systems & Virtualization Security and Cyber-Physical Systems Security (if applicable). Skills include creating detailed architecture specifications, designing for cloud platforms, applying Zero Trust principles, interpreting risk assessments, and thinking like an adversary. Abilities include judging the relative importance of requirements and being able to credibly defend design decisions. In CBK banking and financial sector, this means designing secure cloud architectures for financial services and applying strong security principles to critical banking infrastructure.

Security Architecture
Level 3: Expert
Holds titles like Chief Security Architect or Chief Cloud Security Architect. Focuses on enterprise-level security architecture. Works with enterprise architects to develop the overall information security architecture. Defines standard solutions, develops methodologies, templates, and frameworks. Understands the security advantages and vulnerabilities of common products and technologies. May progress to a Chief Information Officer or CISO role.
Knowledge, Skills, and Abilities
Requires deep core knowledge in Secure Software Lifecycle and Cyber-Physical Systems Security, and wider knowledge in Network Security. Skills involve developing enterprise security architecture, interpreting security policies into architectural solutions, applying common architectural frameworks (TOGAF, SABSA), and designing robust security mechanisms. Abilities include integrated thinking across business, security, and regulatory constraints. In CBK banking and financial sector, this involves defining the overall security architecture strategy for the bank's IT landscape, including payment systems and customer platforms, ensuring legislative compliance.

SUGGESTED QUALIFICATIONS

Relevant qualifications cover Secure Software Lifecycle, System Security concepts, and Architectural frameworks. The sources suggest that expertise often comes from deep IT and cybersecurity knowledge rather than direct transferable skills from unrelated fields. Qualifications demonstrating expertise in security architecture principles, cloud security design, and specific technologies (e.g., PKI) would be relevant. Certifications like CISSP-ISSAP, SABSA, or cloud security architect certifications would be beneficial.

4. SECURITY OPERATIONS

Secure Operations manages an organization's information systems, networks, and processes according to security standards and requirements. The primary goal is to protect against attacks and accidental security incidents by following formal secure operating procedures and monitoring security controls. Responsibilities include managing alerts which may represent unauthorized entry to a system or potential nefarious activity, monitoring system performance and security metrics, ensuring effective system processes like backups, managing development/test environments, and applying updates quickly and safely. With experience, this role involves overseeing overall system security and performance, planning work for colleagues, setting operational standards, and selecting/implementing monitoring tools. Secure

Operations is considered a good lateral movement into a cybersecurity career, particularly for those with IT system operator or administrator experience. In CBK banking and financial sector, this involves managing the secure day-to-day operations of critical financial systems, platforms, and networks, ensuring data protection and access controls are strictly enforced.

Secure Operations
Level 1: Specialist
Focuses on operating systems and networks according to established security policies and procedures. Manages access controls, monitors system performance, ensures compliance of processes like backups, applies patches, and supports users with data access. May perform first line security monitoring and analysis using SIEM technologies.
Knowledge, Skills, and Abilities
Requires solid understanding of Operating Systems & Virtualization Security and Network Security is important. Skills include configuring/managing servers and network devices, monitoring performance and security, applying patches, and managing access controls. Abilities include attention to detail, working in a structured way, and troubleshooting. In CBK banking and financial sector, this involves securely managing servers and networks handling financial data and transactions, implementing strict access controls for sensitive financial information.

Secure Operations
Level 2: Senior Specialist
Responsible for the overall performance and security of live systems. Plans and sets priorities for colleagues. Sets and monitors compliance with operational security standards. Selects and implements performance and security monitoring tools. May manage an IT helpdesk.
Knowledge, Skills, and Abilities
Needs to apply core knowledge more broadly and deeply. Skills include selecting/implementing monitoring tools, change management, establishing/monitoring compliance, and potentially IT helpdesk management. Abilities involve working across multiple functions and collaborating effectively. In CBK banking and financial sector, this means ensuring the secure operation of critical banking platforms, managing change processes for financial systems, and monitoring security metrics for financial operations.

Secure Operations
Level 3: Expert
Holds titles like IS Operations & Security Manager. Oversees multiple Secure Operations functions. Focuses on establishing processes for maintaining security throughout the information lifecycle. Coordinates security activities across the organization. Assesses and responds to new technical, physical, personnel, or procedural vulnerabilities. May manage a Security Operations Centre (SOC) or Network Operations Centre (NOC).
Knowledge, Skills, and Abilities
Requires understanding of Cyber-Physical Systems Security (if applicable), Distributed Systems Security, and Human Factors. Skills include establishing processes for maintaining security throughout the information lifecycle, coordinating security activities, and managing vulnerability remediation. Abilities involve leadership and managing complex operations. In CBK banking and financial sector, this could include overseeing the security of systems involved in payment processing or trading platforms, ensuring resilience and strict adherence to operational security procedures.

SUGGESTED QUALIFICATIONS

Relevant qualifications cover Security Operations, Endpoint Security Solutions, Operating Systems & Virtualization Security, and Network Security. Experience as a system operator or administrator is a good foundation. Qualifications demonstrating proficiency in specific operating systems (Windows Server, Linux), network management, SIEM technologies (Splunk, LogRhythm), and security operations best practices would be relevant. Certifications like Security+, CompTIA CySA+, or vendor-specific certifications for security platforms are useful.

5. CYBER THREAT INTELLIGENCE

Cybersecurity Threat Intelligence (CTI) is the assessment, validation, and reporting of information on current and potential cyber threats to maintain an organization's situational awareness. This guides decision-making by providing assessments underpinned by rigorous analysis. CTI professionals use specialist tools to curate intelligence feeds, interpret information to understand emerging and developing threats, and work closely with vulnerability management teams. They research threats, Indicators of Compromise (IoCs), and threat actor Tactics, Techniques and Procedures (TTPs). In the event of an incident, CTI supports the response by analyzing the attack and potentially attributing it to an external actor. This may involve sharing intelligence with other organizations or government agencies. In the banking and financial sector, intelligence sharing is common to protect the whole sector. CTI is critical for focusing resources on addressing specific risks faced by the organization.

Cybersecurity Threat Intelligence (CTI)
Level 1: Specialist
Supports the delivery of cybersecurity assessments and recommendations. Research threats, IoCs, and TTPs to support Threat Hunting, Signature Development, and Threat Intelligence Platform (TIP) processes. Evaluates and refines technical intelligence feeds. Works closely with vulnerability management teams. May act as part of the Incident Response team during incidents.
Knowledge, Skills, and Abilities
Knowledge of Malware & Attack Technologies, Security Operations & Incident Management, Network Security, and Forensics. Skills include analytical tradecraft, intelligence analysis, handling open-source intelligence (OSINT), and applying formal methodologies (Kill Chain, MITRE ATT&CK, Diamond Model). Abilities involve rigorous analysis and interpretation of data. In CBK banking and financial sector, this means analyzing malware targeting financial systems, understanding attack vectors used against banks, and applying frameworks to track threats.

Cybersecurity Threat Intelligence (CTI)
Level 2: Senior Specialist
Leads the delivery of cybersecurity assessments and recommendations to technical, managerial, and executive stakeholders. Maintains detailed threat actor profiles. Establishes mutual technical intelligence sharing with credible external sources. Identifies research gaps and opportunities. May become a subject matter expert in Advanced Persistent Threat (APT) groups or adversaries' TTPs.
Knowledge, Skills, and Abilities
Needs deeper expertise in core knowledge areas to assimilate understand complex multi-faceted threat vectors. Skills include subject matter expertise on specific threat actors or TTPs, evaluating intelligence relevance and reliability, processing and collating data to maintain situational awareness, and predicting/prioritizing threats using tools like MITRE ATT&CK Navigator. Abilities involve using analytical skills to interpret complex information and communicate findings effectively. In CBK banking and financial sector, this involves tracking sophisticated financial crime groups (APTs) and their methods, predicting risks to the bank's assets, and sharing actionable intelligence within the banking and financial sector.

Cybersecurity Threat Intelligence (CTI)
Level 3: Expert
Holds titles like Senior/Lead Cyber Threat Intelligence Manager or Director of Security Operations. Oversees the CTI function. Directs the assessment and validation of threat information. Defines the intelligence needs and reporting requirements for the organization, ensuring assessments guide strategic decision-making. Likely manages a team of CTI professionals.
Knowledge, Skills, and Abilities
Requires broad knowledge across multiple areas to provide context for the work. Skills include directing the intelligence process, ensuring the accuracy and timeliness of reporting, and integrating threat intelligence into risk management and security operations. Abilities involve strategic thinking, leadership, and effectively disseminating intelligence reports to varied audiences. In CBK banking and financial sector, this means setting the strategic direction for threat intelligence collection and analysis, ensuring the bank is prepared for threats targeting the banking industry, and advising executive management on the cyber threat landscape.

SUGGESTED QUALIFICATIONS

Relevant qualifications cover Threat Intelligence, Malware & Attack Technologies, Security Operations & Incident Management, and Forensics. The sources mention that prior experience in intelligence analysis in fields like police or military services is a good foundation. Qualifications demonstrating proficiency in intelligence analysis methodologies, OSINT tools, and threat modeling frameworks would be relevant. Certifications like GCTI, CISSP, or CREST Certified Threat Intelligence Manager would be useful.

6. VULNERABILITY ASSESSMENT

Vulnerability Assessment (VA) involves managing the configuration of protected systems to ensure that any vulnerabilities are understood and managed. This is an essential role focused on protecting information systems and assets by identifying and closing off vulnerabilities in devices, systems, and networks. Activities include staying updated on vulnerabilities in software and hardware, researching potential vulnerabilities in the organization's systems, identifying, and prioritizing them, and proposing and implementing mitigations. VA professionals often run network and application vulnerability scans using specialist tools. They may work on projects related to patch compliance and sector-specific compliance (like PCI-DSS). With more experience, they interpret scan results, get involved in incident response to understand root causes, and help develop security initiatives. In CBK banking and financial sector, VA is critical for identifying and remediating vulnerabilities in applications, infrastructure, and systems that handle sensitive customer and financial data, ensuring compliance with strict security standards.

Vulnerability Assessment (VA)
Level 1: Specialist
Assists in looking for potential vulnerabilities, conducts and interprets vulnerability scans. Uses investigative and analytical skills. Runs network and application vulnerability scans. Stays updated with vulnerability reports. May support clients on vulnerability issues. Operates network intrusion detection and other security systems.
Knowledge, Skills, and Abilities
Skills include interpreting, analyzing, and reporting security events, using network and application scanning tools (Nessus, Burp Suite, NMAP), configuring/troubleshooting networks, and maintaining asset databases. Abilities include an inquisitive nature, problem-solving, prioritization, and effective communication. In CBK banking and financial sector, this means using scanning tools to identify vulnerabilities in banking applications and infrastructure, prioritizing them based on potential impact to financial data and services, and reporting findings accurately.

Vulnerability Assessment (VA)
Level 2: Senior Specialist
Conducts and interprets complex vulnerability scans. Identifies and prioritizes vulnerabilities. Proposes and implements mitigations. Works on compliance projects (e.g., PCI-DSS). Gets involved with incident response teams to identify root causes and lessons learned. Drives fundamental change by developing security initiatives. May become a Senior/Lead Threat and Vulnerability Analyst.
Knowledge, Skills, and Abilities
Needs wider knowledge in Risk Management and Governance. Skills involve assessing new vulnerabilities, investigating solutions, recommending controls, managing patching and remediation efforts, and potentially configuring encryption protocols. Abilities include interacting effectively with technical and non-technical teams. In CBK banking and financial sector, this includes managing the remediation lifecycle for vulnerabilities in critical financial systems, ensuring patch compliance with security policies, and working with internal/external auditors on vulnerability findings.

Vulnerability Assessment (VA)
Level 3: Expert
Oversees the Vulnerability Management program for the organization. Establishes processes for routine vulnerability assessments and remediation tracking. Works with Certifying Authorities (CA). May manage a team of vulnerability analysts. Ensures that the organization's vulnerability posture aligns with risk appetite and regulatory requirements. Might progress to a Security Operations Centre manager role.
Knowledge, Skills, and Abilities
Requires expertise in Secure Operations & Service Delivery principles. Skills include establishing and maintaining Security Operating Procedures related to vulnerability management, coordinating penetration testing, assessing and responding to vulnerabilities, and managing the implementation of Information Security programs related to VA. Abilities involve leadership and strategic thinking in managing vulnerability risk. In CBK banking and financial sector, this means defining the bank's strategy for vulnerability management, ensuring controls are in place to mitigate risks to financial assets, and coordinating vulnerability assessment activities across the organization.

SUGGESTED QUALIFICATIONS

Relevant qualifications cover Security Operations & Incident Management, Network Security, and potentially Security Testing. Experience in roles involving research, analysis, and sharing findings is helpful. Qualifications demonstrating proficiency with vulnerability scanning tools, network configuration, and understanding of exploit techniques would be relevant. Certifications such as CompTIA Security+, CompTIA CySA+, EC-Council CEH, or vendor-specific certifications for VA tools are useful.

7. DIGITAL FORENSICS & INCIDENT RESPONSE

Digital Forensics and Incident Response (DFIR) is a combined specialism that involves preparing for, handling, and following up on cybersecurity incidents to minimize damage and prevent recurrence, as well as the technical process of identifying and reconstructing events on IT systems. Incident Response focuses on understanding what is happening during an incident, stopping the attack, and analyzing causes to prevent future occurrences. Digital Forensics involves delving deep into hardware and software using specialized tools to recover and analyze data from systems and devices. This includes collecting evidence, analyzing malicious software, and producing formal reports. DFIR professionals work methodically and carefully, whether as part of a forensics team, collaborating with other specialists, or supporting law enforcement. In a corporate environment, particularly in banking, DFIR examines breaches to understand exploited vulnerabilities, damage caused, and attacker identity to enhance security controls. The ability to be effective and action-oriented while remaining calm and collaborative is crucial.

Digital Forensics and Incident Response (DFIR)
Level 1: Specialist
Participates in incident handling and digital forensics investigations. Triages devices, uses tools to retrieve data (including imaging). Analyzes files, data elements, and memory for evidence. Handles materials carefully to avoid contamination. Logs significant actions. Monitors network/system activity to identify anomalies. May be a SOC Analyst.
Knowledge, Skills, and Abilities
Core knowledge in Security Operations & Incident Management is key. Related knowledge in Malware & Attack Technologies and Adversarial Behaviors is important. Skills include file system/memory analysis, using common forensics tools (UFED, EnCASE, FTK), and scripting. Abilities involve problem-solving, logical thinking, and remaining calm under pressure. In CBK banking and financial sector, this means collecting and analyzing digital evidence from systems involved in financial fraud or breaches, ensuring chain of custody is maintained for potential legal proceedings.

Digital Forensics and Incident Response (DFIR)
Level 2: Senior Specialist
Takes a leading role in security incidents and digital forensics investigations. Analyzes malicious software to understand attack techniques and attribute activity. Produces formal reports suitable for evidential submission. Defines and implements processes for detecting and investigating incidents. Carries out investigations using relevant information sources. Assesses the need for forensic activity and coordinates specialists. May be a Senior Digital Forensic Investigator or Senior Cyber Incident Response Analyst.
Knowledge, Skills, and Abilities
Needs deeper technical skills like software analysis (possibly with decompilers) and physical disassembly of devices. Skills include coordinating response activities and writing formal reports suitable for submission in legal proceedings. Abilities include action-orientation and collaboration. In CBK banking and financial sector, this involves leading investigations into complex breaches affecting financial data, analyzing sophisticated malware used in attacks, and producing detailed reports for internal stakeholders and potentially law enforcement.

Digital Forensics and Incident Response (DFIR)
Level 3: Expert
Holds titles like Manager, Digital and Forensic Investigations or Forensic Lead. Manages a DFIR team or a Security Operations Centre (SOC). Establishes and maintains a Computer Security Emergency Response Team (CSIRT) or similar. Oversees the investigation capability, including when third parties are involved. Ensures adherence to legal guidelines and evidential standards. May appear as an expert witness.
Knowledge, Skills, and Abilities
Requires broader knowledge including Network Security, Web & Mobile Security, and Human Factors. Skills involve defining incident management processes, establishing response teams, and presenting evidence. Abilities include leadership and managing a team through high-pressure situations. In CBK banking and financial sector, this means overseeing the bank's response to major cybersecurity incidents affecting customer funds or services, managing forensic investigations into large-scale fraud, and ensuring the team is equipped to handle evolving threats.

SUGGESTED QUALIFICATIONS

Relevant qualifications cover Forensics, Incident Management, and relevant Law & Regulation. This specialism often requires advanced, specialized skills gained through training rather than direct transfer from many other careers. Qualifications demonstrating expertise in specific forensic tools, operating system/network analysis, malware analysis, and incident handling procedures would be relevant. Certifications like SANS GIAC (GCIH, GCFA, GNFA), EnCase Certified Examiner (EnCE), or CREST Certified Incident Responder are highly valuable.

8. IDENTITY AND ACCESS MANAGEMENT

Identity and Access Management (IAM) is the management of policies, procedures, and controls to ensure that only authorized individuals access information or computer-controlled resources. This is an essential part of day-to-day operations, particularly vital in larger organizations like banks with significant amounts of sensitive commercial and client information. IAM professionals manage user identities, authentication technologies, and authorization rules across isolated and distributed systems. They apply principles like Least Privilege and Separation of Duties and are involved in auditing user access. With experience, IAM professionals work with industry-standard protocols and solutions and provide expert advice to senior stakeholders. IAM often involves detailed, methodical work and the application of security rules. In CBK banking and financial sector, IAM is paramount for securing access to customer accounts, internal financial and banking systems, and sensitive data, ensuring compliance with regulations and preventing unauthorized access or fraudulent activity.

Identity and Access Management (IAM)
Level 1: Specialist
Focuses on applying security rules and following detailed, methodical procedures. Administers logical and physical user access rights. Securely configures and maintains equipment in accordance with security policies. May support identity and access management processes. Monitors processes for policy violations.
Knowledge, Skills, and Abilities
Requires a very good understanding of Authentication, Authorization & Accountability and Web & Mobile Security. Solid understanding of Operating Systems & Virtualization Security. Skills include administering user access rights, configuring equipment securely, and monitoring policy violations. Abilities include attention to detail and methodical work. In CBK banking and financial sector, this means managing user access to banking applications and systems, applying security configurations to devices handling financial data, and monitoring for anomalous access patterns.

Identity and Access Management (IAM)
Level 2: Senior Specialist
Applies Authentication & Authorization principles and processes. Implements industry standard IAM protocols (Kerberos, OAuth, FIDO, SAML, LDAP) and solutions (Okta, Auth0, Active Directory). Applies security principles like Least Privilege and Separation of Duties. Audits user and process access, including interpreting system logs. Provides expert advice and analysis to senior stakeholders. Works and influences cross-functionally. May be an Identity & Access Management Specialist.
Knowledge, Skills, and Abilities
Skills involve applying industry standard IAM protocols and solutions, applying security principles (Least Privilege, Separation of Duties), and auditing access logs. Abilities include providing expert advice and influencing others. In CBK banking and financial sector, this includes implementing multi-factor authentication (MFA) and privileged access management solutions for critical financial systems, auditing access to customer data, and ensuring compliance with data protection regulations (like GDPR or CCPA). Needs a solid understanding of Risk Management and Governance and Privacy and Online Rights in relation to the impact on IAM.

Identity and Access Management (IAM)
Level 3: Expert
Holds titles like Cyber Manager - Identity & Access Management or Director. Directs, oversees, and designs the organization's IAM structures, policies, procedures, and controls. Ensures compliance with legal and regulatory requirements related to identity and privacy. May progress within the specialism to become a Chief Data Protection Officer.
Knowledge, Skills, and Abilities
Requires wider knowledge beyond IAM and should include Security Architecture. Skills involve directing and overseeing enterprise-level IAM governance, ensuring compliance with legal and regulatory requirements related to identity and privacy, and integrating IAM with overall security strategy. Abilities include strategic thinking and managing complex access control systems across the organization. In CBK banking and financial sector, this means establishing the bank's enterprise IAM strategy to protect customer identities and financial assets, ensuring global regulatory compliance, and overseeing the secure management of all access points to banking infrastructure.

SUGGESTED QUALIFICATIONS

Relevant qualifications cover Authentication, Authorization & Accountability, Web & Mobile Security, Operating Systems & Virtualization Security, and Cryptography. Qualifications demonstrating proficiency with IAM protocols and solutions, access auditing, and identity management concepts would be relevant. Certifications like CompTIA Security+, CISSP (especially with the Access Control domain), vendor-specific certifications for IAM products (e.g., Microsoft Identity), or certifications related to privacy (e.g., CIPP/E) are useful.

9. EMERGING TECHNOLOGY

Emerging Technology in the banking and financial sector involves researching, evaluating, designing, and implementing cutting-edge technologies like Artificial Intelligence (AI), Machine Learning (ML), Quantum Computing, Quantum-Safe Cryptography, Blockchain, and advanced Cloud Computing to enhance security, efficiency, and introduce new services. This specialism is critical for banks aiming to innovate securely, stay competitive, and meet the modernization goals often outlined in Kuwait Vision 2035. Professionals in this area must understand the security implications of new technologies from their inception, collaborate with various technical and business teams, and often align implementations with national strategic priorities and regulatory requirements. This role requires a high level of technical expertise, foresight, and the ability to navigate uncertainty in rapidly evolving technological landscapes.

Emerging Technology
Level 1: Specialist
Focuses on researching specific emerging technologies, conducting technical evaluations or proof-of-concept implementations, and supporting the integration of new security components or features into existing systems. May assist in assessing the security posture of new platforms or applications built with emerging tech and contribute to technical documentation.
Knowledge, Skills, and Abilities
Requires knowledge of core cybersecurity domains with a focus on specific emerging technologies (e.g., AI/ML security risks, blockchain, basic quantum concepts). Solid understanding of Secure Software Lifecycle and Network Security. Skills include researching technical concepts, conducting technical tests or evaluations, and documenting findings. Abilities include curiosity, problem-solving, and technical analysis. In banking, this involves understanding how these technologies apply to financial services and their potential security implications.

Emerging Technology
Level 2: Senior Specialist
Takes a leading role in evaluating and designing secure solutions incorporating emerging technologies, such as designing secure blockchain platforms for financial transactions or evaluating the risks of AI in cybersecurity operations. Conducts in-depth security analyses of emerging tech frameworks and recommends implementation strategies. Will manage projects related to emerging tech adoption. Engages with business leaders to explain the potential and risks of new technologies in the banking and financial sector.
Knowledge, Skills, and Abilities
Requires solid knowledge of Secure System Architecture & Design and Risk Management & Governance. Skills involve designing secure architectures for new platforms, conducting detailed risk assessments for emerging tech deployments, evaluating and implementing new security, and communicating complex technical concepts to non-technical stakeholders. Abilities include strategic thinking regarding technology adoption and influencing technical direction. In CBK banking and financial sector, this includes assessing the security risks of AI-driven fraud detection systems or designing the security for a distributed ledger technology (DLT) platform for settlements.

Emerging Technology
Level 3: Expert
Holds a senior strategic role overseeing the bank's adoption and secure integration of emerging technologies across the enterprise. Defines the technical standards and architectural principles for using new technologies securely. Directs research efforts into future technological threats and opportunities (e.g., post-quantum cryptography strategy). Contributes to the bank's long-term technology roadmap and innovation strategy, ensuring alignment with national development goals like Vision 2035.
Knowledge, Skills, and Abilities
Requires extensive knowledge across multiple future technologies, including Cryptography, Secure System Architecture, and Quantum Security. Skills involve defining the strategic direction for technology security, establishing research programs, managing enterprise-wide technology risk, and engaging with industry bodies and regulators on emerging tech standards. Abilities include visionary leadership, complex decision-making integrating business/security/regulatory factors, and driving innovation while managing risk. In CBK banking and financial sector, this means setting the strategic approach for adopting technologies like quantum computing and artificial intelligence.

SUGGESTED QUALIFICATIONS

For AI and ML, certifications like Certified Artificial Intelligence Practitioner (CAIP) and Machine Learning Certification by Stanford University provide essential knowledge. In Quantum Computing, CISSP with a focus on Cryptography and Certified Cybersecurity Professional (CCP) with Quantum Security Specialization offer insights into quantum-safe methods. For Blockchain, certifications such as Certified Blockchain Security Professional (CBSP) and Certified Blockchain Expert (CBE) cover security principles.

7.5 Senior Cyber Leadership Program (SCLP)

Overview of Senior Cybersecurity Leadership

This Senior Cybersecurity Leadership Program (SCLP) is designed to establish a comprehensive and structured approach to developing, managing, and sustaining a skilled and resilient cyber resilience workforce. This framework aims to address the growing demand for cybersecurity professionals cross the Kuwaiti banking and financial sector by providing clear guidelines and strategies for workforce development, talent management, and continuous improvement.

The SCLP is a Sector Wide initiative to build a strong, coordinated cybersecurity leadership ecosystem within the Kuwaiti banking and financial sector. The program aligns with national security goals and aims to prepare decision-makers with the mindset, skills, and strategic capabilities needed to navigate today's complex cyber threat landscape. The key objectives are:

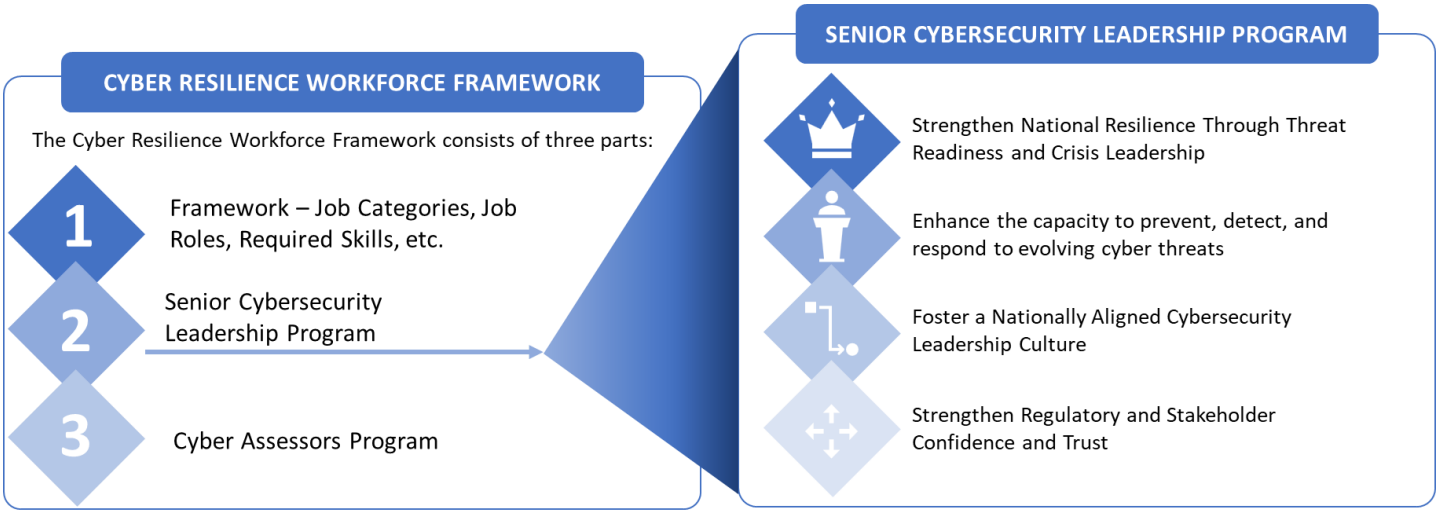
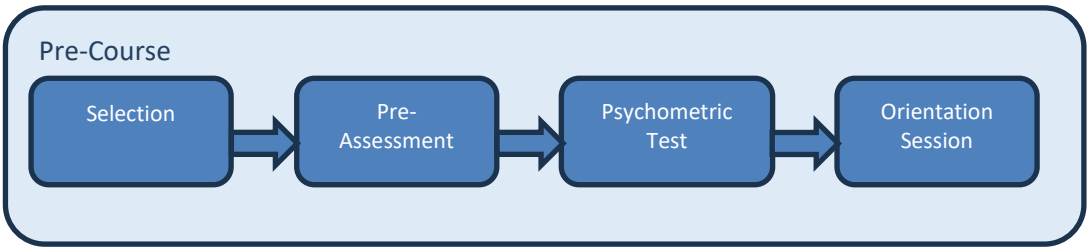


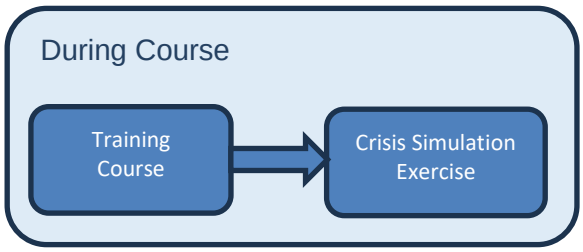
Figure 2. Overview of Senior Cybersecurity Leadership Program

7.5.1 Structure of the Senior Cybersecurity Leadership Program (SCLP)

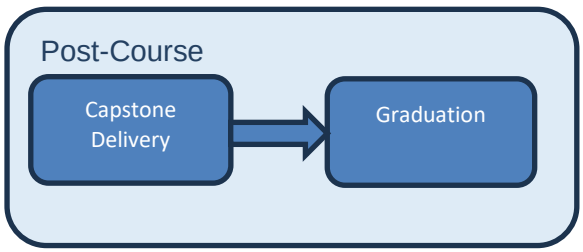
The structure of the SCLP may include some or all elements detailed below. Individual and Sector benefits that may be derived from each element are highlighted.



Senior Cybersecurity Leadership Program (SCLP) – Pre-Course	
(1) Selection	Opt-in selection helps identifies high-potential cybersecurity professionals and decision-makers that are committed to personal growth. **Individual:** Recognizes talent and contributions to date across the sector. **Sector:** Ensures the right people with high commitment commence the program.
(2) Pre-Assessment	Establishes a baseline of cybersecurity knowledge and leadership aptitude. **Individual:** Creates an understanding of areas where personal growth may be sought. **Sector:** Assesses sector-wide readiness and identifies training needs.
(3) Psychometric Test	Measure's cognitive ability, behavioral traits, and leadership potential. **Individual:** Increases self-awareness and adaptive thinking. **Sector**: Encourages well-rounded leadership with emotional intelligence and strategic foresight.
(4) Orientation Session	Introduces the program framework, national objectives, and sectoral priorities. **Individual:** Aligns personal goals with program outcomes, ensuring they are ready for the journey. **Sector:** Builds shared understanding and commitment across institutions.



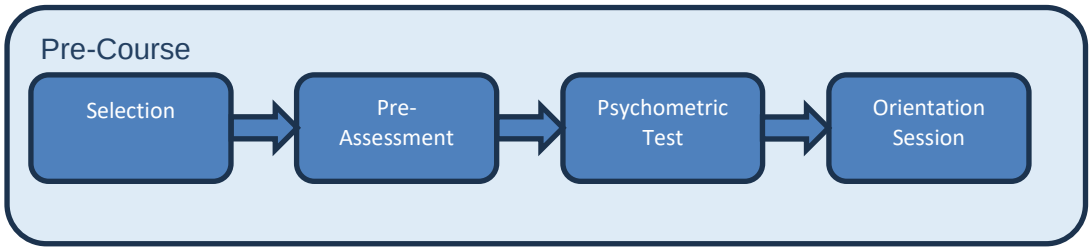
Senior Cybersecurity Leadership Program (SCLP) – During Course	
(5) Training Course	Covers key domains: Threat intelligence, GRC, risk mitigation, crisis response, and strategic leadership. **Individual:** Gains practical and strategic cybersecurity knowledge, skills, and abilities. **Sector:** Builds a cadre of skilled leaders capable of responding to dynamic cyber threats.
(6) Crisis Simulation Exercise	Realistic cyber crisis simulation to test application of skills and decision-making. **Individual:** Demonstrates readiness under pressure and integrate learning. **Sector:** Validates operational effectiveness and cross-sector coordination during incidents.



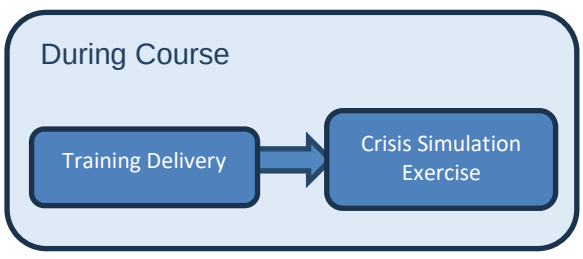
Senior Cybersecurity Leadership Program (SCLP) – Post-Course	
(7) Capstone Delivery	Summative project to help demonstrate growth and problem-solving capabilities, and post-assessment. **Individual:** Demonstrate real-world problem-solving capability in a complex environment. **Sector:** Solving real-world issues experience in Kuwait help strengthen the sectors resilience.
(8) Graduation	Celebration of achievement over the duration of the SCLP. **Individual:** Certified as a cybersecurity leader ready for national-level roles. **Sector:** Alumni strengthens bonds, fostering greater appreciation of each other and improved understanding/cooperation between entities.

7.5.2 Structure of the Senior Cybersecurity Leaders Program (SCLP)

The structure of the CBK current Cybersecurity Leaders Program (SCLP) when built into this format may have two key differences, (1) Crisis Simulation Exercise to be changed out with a more technically focused Cyber Ranges Exercise, and (2) Removal of the Capstone Project



Senior Cybersecurity Leaders Program (SCLP)– Pre-Course	
(1) Selection	Opt-in selection helps identifies high-potential cybersecurity professionals and decision-makers that are committed to personal growth. **Individual:** Recognizes talent and contributions to date across the sector. **Sector:** Ensures the right people with high commitment commence the program.
(2) Pre-Assessment	Establishes a baseline of cybersecurity knowledge and leadership aptitude. **Individual:** Creates an understanding of areas where personal growth may be sought. **Sector:** Assesses sector-wide readiness and identifies training needs.
(3) Psychometric Test	Measure's cognitive ability, behavioral traits, and leadership potential. **Individual:** Increases self-awareness and adaptive thinking. **Sector**: Encourages well-rounded leadership with emotional intelligence and strategic foresight.
(4) Orientation Session	Introduces the program framework, national objectives, and sectoral priorities. **Individual:** Aligns personal goals with program outcomes, ensuring they are ready for the journey. **Sector:** Builds shared understanding and commitment across institutions.



Senior Cybersecurity Leaders Program (SCLP)– During Course	
(5) Training Delivery	Covers training already agreed through Academy and embedded into the current SCLP. **Individual:** Gains technical skills and abilities underpinned by sound knowledge. **Sector:** Builds strong cyber skills across the Banking and Financial Sector in Kuwait.
(6) Cyber Range Exercise	Realistic Banking and Financial Sector Exercise (CTF, Threat Hunt, Live Fire, etc.) to test application of technical skills. **Individual:** Demonstrates technical aptitude and readiness to tackle complex threats. **Sector:** Provides confidence in cross-sector capability and information sharing channels.

Senior Cybersecurity Leaders Program (SCLP)– Post-Course	
(7) Graduation	Celebration of achievement over the duration of the SCLP. **Individual:** Certified as a cybersecurity leader ready for national-level roles. **Sector:** Alumni strengthens bonds, fostering greater appreciation of each other and improved understanding/cooperation between entities.

7.5.3 CBK Cyber Workforce Management - Program Execution

To ensure that the program is fit-for-purpose, engaging, and leading-edge, a learning approach that blends both tooling and various delivery methods must be used.

TOOLING

Learning Management System

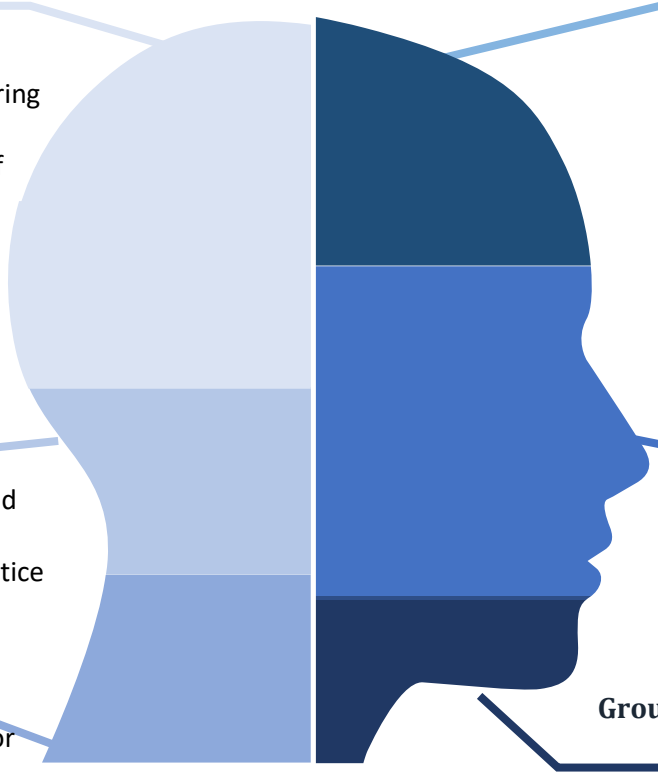
- Provides a central platform for managing and delivering educational content.
- Facilitates the creation, organization, and tracking of courses and training programs.
- Supports interactive learning through quizzes, discussions, and multimedia content.
- Monitors learner progress and performance with analytics and reporting tools.

Simulations / Labs

- Creates lifelike cyber attack scenarios for training and testing purposes.
- Enhances cybersecurity skills through hands-on practice in a controlled environment.

Digital Twin

- Creates a digital replica of physical assets, systems, or processes.
- Uses simulations and analytics to predict future performance and potential issues.



DELIVERY METHODS

Experiential – 50%

- Cyber war games, tabletop exercises, and incident simulation labs.
- Role-play exercises for executive-level crisis communication and board reporting.
- Use case-based learning, not just theory. Include high-impact scenarios like data breaches, regulatory failures, or AI abuse.
- Experiential and Scenario-Based Learning

Theory – 25%

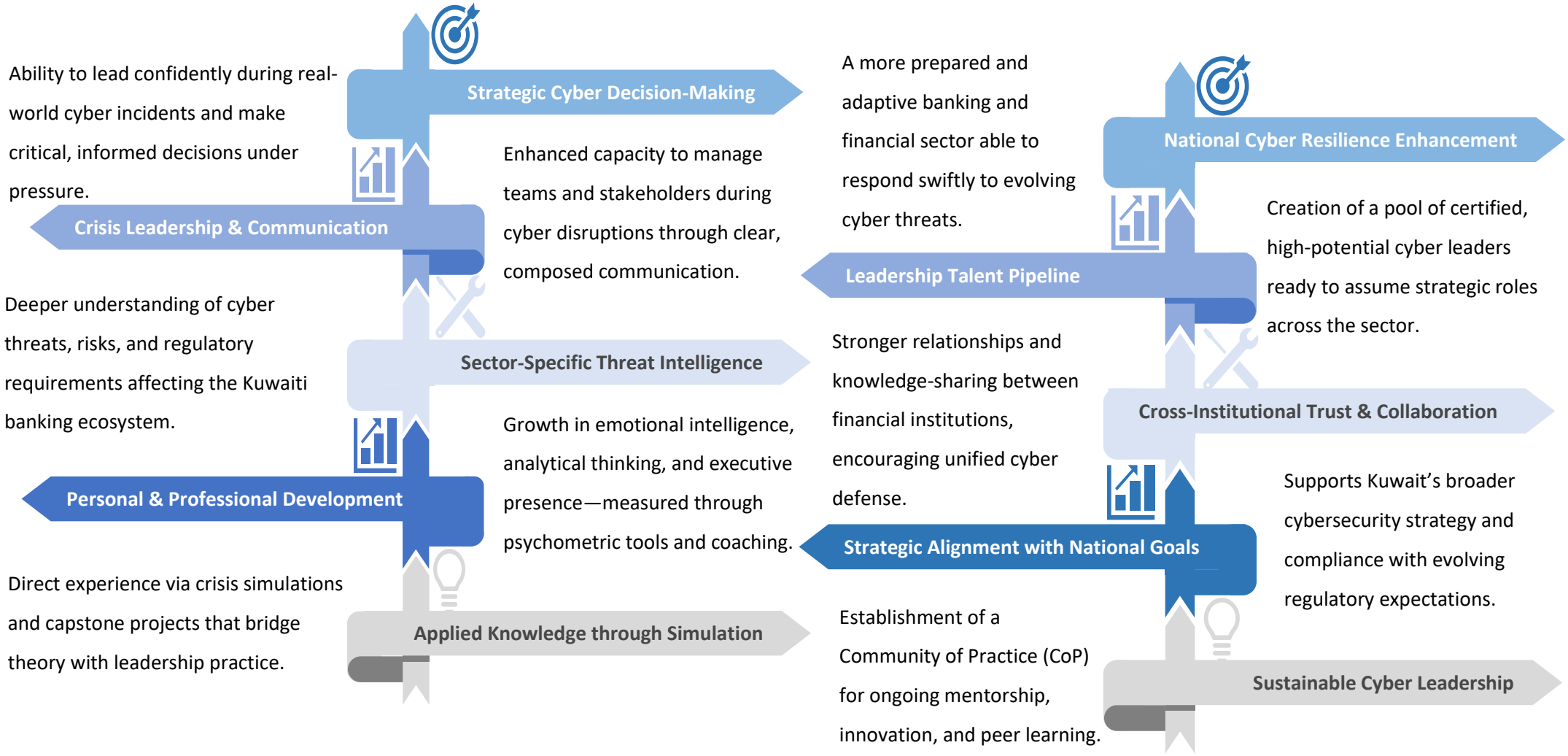
- Instructors must combine deep cybersecurity expertise with experience in banking and executive leadership.
- Ensuring contextual alignment with Arabic/English materials and relevance to Gulf regulatory environments.

Group Collaboration – 25%

- Capstone Project solving a complex problem that the banking and financial sector collectively experiencing.
- Conducted in small groups of 3-4 people.

7.5.4 CBK Cyber Workforce Management - Learning Outcomes

Upon completion of the Cybersecurity Leadership Program, delegates will achieve the following attributes. These individual outcomes lead to wider sector cyber maturity and resilience.



7.5.5 Senior Cybersecurity Leadership Program – KPI Framework

To help measure the effectiveness of the SCLP, demonstrate value from the initiative, and to implement continuous improvement, several Key Performance Indicators (KPIs) must be identified and tracked. Below provides some of the important KPIs that the program should capture.

Table 4: Cybersecurity Leadership Program – KPI Framework

KPI ID	DESCRIPTION	GOAL
1. Training Delivery and Completion		
KPI 1.1	% of targeted executives and senior leaders enrolled in the training	> 50%
KPI 1.2	% of enrolled participants who complete the program	>95%
KPI 1.3	% of participants completing Capstone Exercise on time	>95%
2. Knowledge and Skills Acquisition		
KPI 2.1	% increase in cybersecurity knowledge from pre- to post-training (using assessment)	>30%
KPI 2.2	% of participants scoring above 80% on the Capstone Exercise	>70%
3. Behavioural Change and Application		
KPI 3.1	% of leaders reporting increased confidence in cyber decision-making (via post-training survey)	>80%
4. Organizational Impact		
KPI 4.1	# of leadership-driven cybersecurity initiatives implemented within 6 months post-training	> # of attendees
KPI 4.2	# of successful incident response simulations led or participated in by trained leaders	> # of attendees
KPI 4.3	% reduction in critical audit findings attributable to governance gaps	>50%
5. Program Feedback and Satisfaction		
KPI 5.1	Overall participant satisfaction rate	>90%

KPI 5.2	% of participants who would recommend the training to peers	>90%
KPI 5.3	% of feedback incorporated into program improvements	>95%
6. Strategic and Sectoral Alignment		
KPI 6.1	% alignment of program content with CBK cybersecurity framework and Kuwait Vision 2035	>95%
KPI 6.2	# of sector-level leadership forums or working groups attended by program alumni	> # of attendees
KPI 6.3	# of trained leaders contributing to national or sectoral cyber resilience initiatives	> # of attendees

7.6 Cyber Assessor Program (CAP)

Overview of Cybersecurity Assessors Program

This **Cybersecurity Assessors Program (CAP)** is designed to equip cyber auditors with the necessary knowledge and practical skills to enable them to assess and ensure compliance with the Central Bank of Kuwait (CBK) Cybersecurity and Operational Resilience Framework (CORF), PCI-DSS, and other relevant global and regional banking regulations. The course leverages the CORF to help auditors evaluate regulated entities' security posture, risk management, and incident response capabilities. Ultimately, it aims to foster a culture of continuous improvement and regulatory alignment within Kuwait's banking and financial sector.

The CAP is tailored for individuals serving as Independent Competent Assessors (such as CBK approved consultancies) who require a comprehensive understanding for the CORF to undertake Audits in a consistent manner, the Information Security Team within CBK who will conduct spot checks on banks, and the Internal Auditor of the Regulated Entities acting as their third line of defense. The key objectives are:

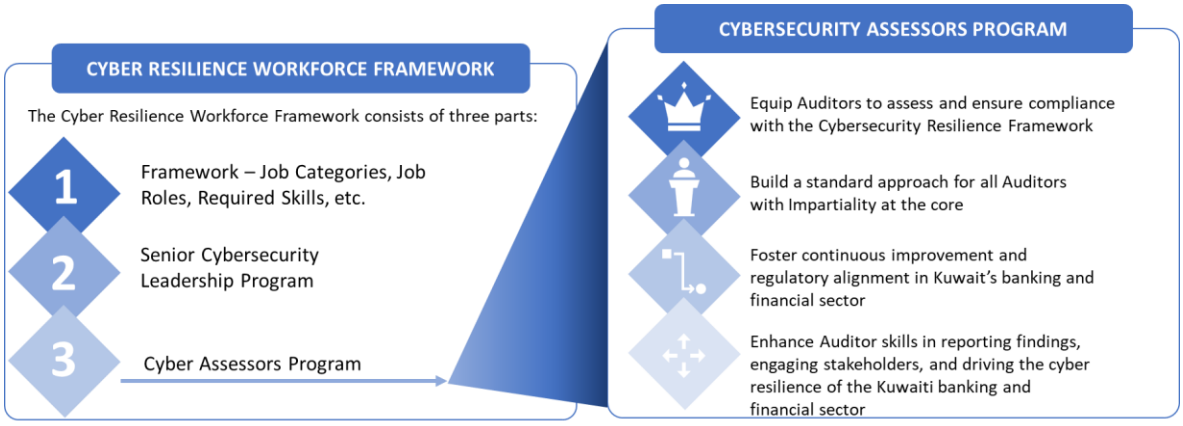


Figure 3. Overview of Cybersecurity Assessors Program

Benefits & Objectives

This **Cybersecurity Assessors Program (CAP)** has been designed to focus on three specific personas. Each of the personas is eligible to attend the CAP. For Independent Competent Auditors, it is mandatory if intending to conduct a formal CBK CORF Audit.

1. Independent Competent Auditor
• Provides formal audit capability to the Kuwaiti banking and financial sector. • Provides expert, objective audits across the sector. • Provides consistency and impartiality throughout.

2. CBK Cyber Inspection Team
• Provides a 'spot check' capability on regulated entities. • Focuses on specific areas to help ensure technical compliance. • Strengthens regulatory enforcement of CORF.

3. Regulated Entity Internal Audit & Cyber Risk
• Gain essential knowledge on CORF to assist compliance across org. • Enables them as an impartial internal resource for Audit preparation. • Strengthens internal control environment and 3rd Line of Defense.

To ensure that personnel are suitable qualified to conduct CORF audits as any of the three personas, they will need to ensure they meet several criteria. Those are:

	Criteria
1	Sound understanding of the Cybersecurity Resilience Framework, its structure, definitions, maturity ratings, and the ultimate intent of the CORF.
2	A strong understanding of cybersecurity tools, technologies and best practices is essential to ensure correct assessment of control implementation effectiveness.
3	Mature knowledge of the Kuwaiti Banking and Financial Sector to allow contextualization of controls and how they relate to the regulatory landscape.
4	Well-developed analytical skills to evaluate complex systems, identify vulnerabilities, and assess risk. Critical thinking allows them to interpret audit findings accurately and prioritize issues based on impact.

5	Effective communications skills to clearly communicate their findings and recommendations to both technical and non-technical stakeholders, ensuring audit results are understood and actionable.

Note: Assessment Criteria - Participants' understanding and skills are assessed through knowledge checks, practical labs, case studies, role-play/simulation, and a final assessment. To ensure currency, the CAP Certificate will be valid for 2-years, after which the Auditor must retake the assessment.

Success Factors for Training CBK Cyber and Operational Resilience Framework Assessors

1. Alignment with CBK Standards & Resilience-Based Approach	2. Competency-Based Curriculum Design
• Training must fully map to the CBK Cybersecurity Framework, including controls, maturity levels, and domains / sub-domains (e.g., Cyber Risk Management, Email Security, Third-Party Risk management, Cloud Security). • Teach auditors how to link compliance with resilience-based evaluation and resilience outcomes, not just checklist adherence.	• Cyber risk assessment. • Control evaluation (technical and process-level). • Interview and evidence gathering. • Maturity scoring against CBK benchmarks. • Integrate frameworks like NIST CSF & ISO/IEC 27001

3. Practical Case-Based Learning	4. Simulation of Maturity Assessments
• Use realistic audit scenarios from the banking and financial sector (e.g., evaluating third-party risk, or SOC readiness). • Include red-teaming case reviews, walkthroughs, mock audit interviews, and evidence sampling techniques.	• Scoring maturity levels per domain (e.g., Initial to Innovative). • Articulating rationale and evidence backing their scores. • Benchmarking bank posture against sector averages.

5. Integration with Regulator Expectations	6. Instructor Expertise and Peer Learning
• Include mock regulator-facing activities (e.g., presenting findings to CBK or board audit committees). • Teach how to interpret and apply CBK-mandated audit templates and cyber incident reporting thresholds	• Use experienced cyber auditors, regulators, and banking CISOs as instructors. Experts with GCC cyber regulatory and audit experience- CBK-accredited trainers or ex-bank auditors. • Encourage cross-bank peer dialogue to share practical challenges and sector trends.

7. Ongoing Certification and Recertification	8. Vision 2035 & Emerging Tech Considerations
• Link training to recognized certifications (e.g., CISA, CRISC, GIAC-GSNA). • Require annual refreshers and updates aligned with CBK circulars and emerging threat trends. • Formal certification lapses after 2-years and must be retaken to remain eligible to conduct audits.	• Align training with Vision 2035 goals, focusing on cybersecurity's role in digital banking, fintech, and AI services. • Train auditors to assess AI/ML security, data integrity, APIs, and Open Banking architectures. • Govern collaboration endorsed by CBK, CAIT, and MGRP, supporting workforce development. • Include guest lectures or simulation audits with CAIT and KDIPA to foster public-sector innovation.

Module Breakdown

This Cybersecurity Assessors Program (CAP) is designed as a 5-day course, culminating in a pass/fail assessment to ensure that Auditors are suitably prepared and skilled to conduct audits aligned to the Cyber and Operational Resilience Framework. The high-level modular approach can be found below:

DAY 1		
MORNING	Module 1: Introduction to Cyber and Operational Resilience Framework	This module introduces the Cyber Resilient Framework, focusing on its application within the banking and financial sector in Kuwait. Participants will gain an understanding of the framework's structure, objectives, and regulatory context.

AFTERNOON	Module 2: Essential Technical Skills for Auditors	This module covers the fundamental technical skills required for effective cyber auditing. Participants will learn how to evaluate security controls, conduct vulnerability assessments, and analyze threat intelligence.
DAY 2		
MORNING	Module 3: Soft Skills for Effective Auditing	This module focuses on the soft skills necessary for successful auditing. Participants will learn how to communicate effectively, manage conflicts, and maintain impartiality.
AFTERNOON	Module 4: Case Study Analysis: Banking and Financial Sector	This module involves analyzing real-world case studies from the banking and financial sector. Participants will learn how to apply the Cyber and Operational Resilience Framework to practical scenarios.
DAY 3		
MORNING	Module 5: Risk Management and Compliance	This module covers the principles of risk management and compliance within the Cyber and Operational Resilience Framework. Participants will learn how to evaluate and ensure adherence to cybersecurity policies and regulatory requirements.
AFTERNOON	-Module 6: Effective Reporting and Documentation	This module focuses on the skills required for effective reporting and documentation. Participants will learn how to create clear, concise, and actionable audit reports.
DAY 4		
MORNING	Module 7: Ethical Considerations in Cyber Audit	This module emphasizes the importance of ethics and impartiality in cyber auditing. Participants will learn how to maintain objectivity and fairness throughout the assessment process.
AFTERNOON	Module 8: Advanced Auditing Techniques	This module covers advanced auditing techniques and methodologies. Participants will learn how to conduct in-

		depth assessments and use specialized tools and frameworks.
DAY 5		
MORNING	Module 9: Practical Exercise and Simulation	This module involves practical exercises and simulations to reinforce learning. Participants will engage in hands-on activities to apply their skills in simulated audit scenarios.
AFTERNOON	Cyber Assessors Program Assessment & Certification	This module involves a comprehensive assessment of participants' understanding and application of the Cyber and Operational Resilience Framework. The assessment will include practical exercises, case studies, and a written exam.

Cybersecurity Assessors Program – KPI Framework

To help measure the effectiveness of the CAP, demonstrate value from the initiative, and to implement continuous improvement, several Key Performance Indicators (KPIs) must be identified and tracked. Below provides some of the important KPIs that the program should capture.

Table 5: Cybersecurity Assessors Program – KPI Framework

KPI ID	DESCRIPTION	GOAL
1. Training Delivery, Completion and Outcomes		
KPI 1.1	% of auditors completing the CAP training program on time	> 90%
KPI 1.2	% of auditors attending all training sessions	> 95%
KPI 1.3	% of auditors achieving passing scores in final assessments	> 85%
2. Knowledge and Skills Acquisition		
KPI 2.1	% increase in cybersecurity knowledge from pre- to post-training (using assessment)	> 40%
KPI 2.2	% of participants scoring above 80% on the practical exercises and demonstrating proficiency in CORF, PCI-DSS, and other relevant regulations	> 75%
3. Behavioural Change and Application		
KPI 3.1	% of auditors applying learned skills in real-world scenarios (via post training survey)	> 80%
4. Organizational Impact		
KPI 4.1	% reduction in critical audit findings attributable to governance gaps	> 50%
KPI 4.2	% of auditors involved in cybersecurity policy development	> 40%
5. Program Feedback and Satisfaction		
KPI 5.1	Overall participant auditors' satisfaction rate	> 90%
KPI 5.2	% of participants who would recommend the training to peers	> 85%
KPI 5.3	% of feedback incorporated into program improvements	> 95%

6. Strategic and Sectoral Alignment		
KPI 6.1	% alignment of program content with CBK CORF and Kuwait Vision 2035	> 95%
KPI 6.2	% of trained auditors contributing to national or sectoral cyber resilience initiatives	> 70% of attendees
KPI 6.3	% of auditors certified in AI & cyber audit by 2026	> 60%
7. Compliance & Regulatory Impact		
KPI 7.2	% of regulated entities achieving compliance with PCI-DSS and other relevant regulations	> 80%
KPI 7.3	% reduction in incident response times for regulated entities	> 25%

8. Templates

8.1 SoA Template

SoA Document Control	
Regulated Entity Name	
Regulated Entity Assessor	
Baselines	Cyber Resilience Baselines | OR Baselines | TPRM Baselines
Regulated Entity Reviewer	
Regulated Entity Approver	
Central Bank of Kuwait Reviewer	
Central Bank of Kuwait Approver	

Revision History

Date	Version	Change Reference	Reviewer/ Approver

Cyber Resilience Baselines - SoA						
Domain Ref. No.	**Domain**	**Sub-Domain Ref. No.**	**Sub-Domain**	**Applicability Status [Applicable/Not Applicable]**	**Justification for Non-applicability or Exclusion**	**CBK Comments and Approval**
4	Governance, Risk, and Compliance	4.1	Cybersecurity Governance and Oversight	*[To be filled by the Regulated Entity]*	*[To be filled by the Regulated Entity]*	*[To be filled by CBK]*
4	Governance, Risk, and Compliance	4.2	Cybersecurity Risk Management			
4	Governance, Risk, and Compliance	4.3	Compliance			
4	Governance, Risk, and Compliance	4.4	Independent Audit			
4	Governance, Risk, and Compliance	4.5	Workforce Management			
5	Technology and Operations	5.1	Security Architecture Design			
5	Technology and Operations	5.2	Asset Management			
5	Technology and Operations	5.3	Infrastructure and Network Security			
5	Technology and Operations	5.4	Endpoint and Device Security			
5	Technology and Operations	5.5	Email Security			
5	Technology and Operations	5.6	Identity and Access Management			
5	Technology and Operations	5.7	Cryptography			
5	Technology and Operations	5.8	Application Security and Secure SDLC			
5	Technology and Operations	5.9	Change and Release Management		a	

Cyber Resilience Baselines - SoA						
Domain Ref. No.	Domain	Sub-Domain Ref. No.	Sub-Domain	Applicability Status [Applicable/Not Applicable]	Justification for Non-applicability or Exclusion	CBK Comments and Approval
5	Technology and Operations	5.10	Capacity Management			
5	Technology and Operations	5.11	Data Protection and Privacy			
5	Technology and Operations	5.12	Logging, Monitoring, and Security Incident Management			
5	Technology and Operations	5.13	Cybersecurity Testing and Threat Management			
5	Technology and Operations	5.14	Physical and Environmental Security			
5	Technology and Operations	5.15	Cyber Threat Intelligence			
5	Technology and Operations	5.16	Digital Risk Protection			
6	Third-Party Risk Management and Supply Chain Management	6.1	Third-Party Risk Management (TPRM)			
6	Third-Party Risk Management and Supply Chain Management	6.2	Supply Chain Management			
7	Emerging Technologies	7.1	Advanced Technologies Security			
7	Emerging Technologies	7.2	Cloud Security			
8	Payments Security	8.1	Common Security Controls for Electronic Payment Systems			

Cyber Resilience Baselines - SoA						
Domain Ref. No.	**Domain**	**Sub-Domain Ref. No.**	**Sub-Domain**	**Applicability Status [Applicable/Not Applicable]**	**Justification for Non-applicability or Exclusion**	**CBK Comments and Approval**
8	Payments Security	8.2	Electronic Payment Transaction Monitoring			
8	Payments Security	8.3	Digital Banking Security			
8	Payments Security	8.4	Payment Card Data Security			
8	Payments Security	8.5	Security of Customer Self-Service Machines			
8	Payments Security	8.6	Contactless Payment Technology Security			
9	Operational Resilience	9.1	Business Continuity and Disaster Recovery (BC and DR)			
9	Operational Resilience	9.2	Cyber Crisis Management			

Operational Resilience Baselines - SoA						
Domain Ref. No.	**Domain**	**Sub-Domain Ref. No.**	**Sub-Domain**	**Applicability Status [Applicable/Not Applicable]**	**Justification for Non-applicability or Exclusion**	**CBK Comments and Approval**
3	Governance and Oversight	3.1	Operational Resilience Governance Structure and Oversight	*[To be filled by the Regulated Entity]*	*[To be filled by the Regulated Entity]*	*[To be filled by CBK]*
3	Governance and Oversight	3.2	Operational Resilience Policy and Strategy			
3	Governance and Oversight	3.3	Compliance			
4	Risk and Threat Management	4.1	Risk Assessment Methodology			
4	Risk and Threat Management	4.2	Risk Assessment Process			
4	Risk and Threat Management	4.3	Risk Treatment and Reporting			
5	Business Continuity Management	5.1	Business Impact Analysis			
5	Business Continuity Management	5.2	Recovery Strategies			
5	Business Continuity Management	5.3	Business Continuity Plans (BCP)			
6	Technology Resilience	6.1	Service Management			
6	Technology Resilience	6.2	Backup and Recovery Management			
6	Technology Resilience	6.3	Technology and Resilience Capabilities			
6	Technology Resilience	6.4	Technology Recovery Plans			
6	Technology Resilience	6.5	Cyber Recovery Plans			
7	Third-Party Resilience	-	-			

Operational Resilience Baselines - SoA						
Domain Ref. No.	**Domain**	**Sub-Domain Ref. No.**	**Sub-Domain**	**Applicability Status [Applicable/Not Applicable]**	**Justification for Non-applicability or Exclusion**	**CBK Comments and Approval**
8	Incident and Crisis Management	7.1	Incident and Crisis Management Governance and Planning			
8	Incident and Crisis Management	7.2	Communication and Escalation			
9	Cyber Resilience	-	-			
10	Testing, Training, and Continuous Improvement	9.1	Training, Testing, and Exercising			

TPRM Baselines - SoA						
Domain Ref. No.	**Domain**	**Sub-Domain Ref. No.**	**Sub-Domain**	**Applicability Status [Applicable/Not Applicable]**	**Justification for Non-applicability or Exclusion**	**CBK Comments and Approval**
3	Governance Structure and Oversight	3.1	TPRM Policy and Strategy	*[To be filled by the Regulated Entity]*	*[To be filled by the Regulated Entity]*	*[To be filled by CBK]*
3	Governance Structure and Oversight	3.2	Roles and Responsibilities			
3	Governance Structure and Oversight	3.3	Board and Senior Management Oversight			
3	Governance Structure and Oversight	3.4	Approvals and Periodic Review			

TPRM Baselines - SoA						
Domain Ref. No.	Domain	Sub-Domain Ref. No.	Sub-Domain	Applicability Status [Applicable/Not Applicable]	Justification for Non-applicability or Exclusion	CBK Comments and Approval
4	Risk Management Framework	4.1	Critical Third-Party Service Identification			
4	Risk Management Framework	4.2	Risk Identification and Assessment Methodology			
4	Risk Management Framework	4.3	Dependency Mapping to Critical Processes			
5	Contractual Agreements Considerations	5.1	Contractual Safeguards			
5	Contractual Agreements Considerations	5.2	Legal Binding Agreement			
5	Contractual Agreements Considerations	5.3	Regular Monitoring and Assessment			
5	Contractual Agreements Considerations	5.4	Health Safety and Environment			
5	Contractual Agreements Considerations	5.5	Financial Viability			
5	Contractual Agreements Considerations	5.6	Compliance (Geopolitics, Regulatory, Organizational, Country, and Legal)			
5	Contractual Agreements Considerations	5.7	Corporate Governance			
6	Risk Assessment and Monitoring	6.1	Identification, Assessment, and Mitigation			

TPRM Baselines - SoA						
Domain Ref. No.	Domain	Sub-Domain Ref. No.	Sub-Domain	Applicability Status [Applicable/Not Applicable]	Justification for Non-applicability or Exclusion	CBK Comments and Approval
6	Risk Assessment and Monitoring	6.2	Risk Classification			
6	Risk Assessment and Monitoring	6.3	Ongoing Monitoring of Critical Third Parties			
7	Business Continuity Management and Disaster Recovery	7.1	Business Continuity Plans			
7	Business Continuity Management and Disaster Recovery	7.2	Data Backup and Replication			
7	Business Continuity Management and Disaster Recovery	7.3	Periodic Testing of DR Capabilities			
7	Business Continuity Management and Disaster Recovery	7.4	Recovery and Restoration Procedures			
7	Business Continuity Management and Disaster Recovery	7.5	Business Continuity Management and Recovery			
8	Incident Management	8.1	Incident Detection and Monitoring			
8	Incident Management	8.2	Incident Communication and Escalation Protocols			
8	Incident Management	8.3	Root Cause Analysis			
9	Data Protection and Confidentiality	9.1	Data Encryption and Masking			
9	Data Protection and Confidentiality	9.2	Data Retention and Disposal			

TPRM Baselines - SoA						
Domain Ref. No.	Domain	Sub-Domain Ref. No.	Sub-Domain	Applicability Status [Applicable/Not Applicable]	Justification for Non-applicability or Exclusion	CBK Comments and Approval
9	Data Protection and Confidentiality	9.3	Data Classification and Handling Policies			
10	Sub-Contracting	10.1	Disclosure of Subcontractor and Approval from Regulated Entities			
10	Sub-Contracting	10.2	Monitoring and Oversight			
11	Exit Strategy	11.1	Exit Strategy Planning			
12	Storage of Data	12.1	Data Storage Security			
12	Storage of Data	12.2	Storage Lifecycle Management			
12	Storage of Data	12.3	Data Integrity and Availability			
13	Cross-Border Transaction	13.1	Regulatory and Legal Compliance			
13	Cross-Border Transaction	13.2	Due Diligence and KYC/AML			
13	Cross-Border Transaction	13.4	Secure Data Transfers and Privacy			
13	Cross-Border Transaction	13.5	Monitoring, Reporting, and Audit			
14	Usage of Cloud Services	14.1	Cloud Security			
15	Inter-Affiliates	15.1	Due Diligence and Periodic Review			
15	Inter-Affiliates	15.2	Customer Consent			

TPRM Baselines - SoA						
Domain Ref. No.	**Domain**	**Sub-Domain Ref. No.**	**Sub-Domain**	**Applicability Status [Applicable/Not Applicable]**	**Justification for Non-applicability or Exclusion**	**CBK Comments and Approval**
15	Inter-Affiliates	15.3	Foreign Affiliates			
15	Inter-Affiliates	15.4	Resource Planning			

8.2 Inherent Risk Profiling Template

Tiering Dimension	#	Assessment Criteria	Guidance for Updating Values in the Adjacent Columns	Input to be Provided by the Regulated Entity	Comments -if any- from the Regulated Entity
Total Number of Assets	1	Total balance sheet size (i.e., total number of assets) as of the latest fiscal year.	Numeric value in KWD		
	2.A	Number of assets (other than network devices) which are part of the technology asset inventory; A. Number of Data Centre IT Assets (Servers, Databases, Middleware etc.,).	Permitted values 1 to 50000		
	2.B	B. Number of Portable Devices.	Permitted values 1 to 200000		
	2.C	C. Number of Applications.	Permitted values 1 to 2000		
	3	Number of network devices (firewall, routers, switches, access points, software defined network physical and virtual devices) part of the regulated entity information assets.	Permitted values 1 to 20000		
Market Share	4	Percentage of total domestic banking sector deposits you hold	Percentage		

Tiering Dimension	#	Assessment Criteria	Guidance for Updating Values in the Adjacent Columns	Input to be Provided by the Regulated Entity	Comments -if any- from the Regulated Entity
	5	Percentage of total domestic banking sector loans you hold	Percentage		
	6	Your share of domestic digital payment transaction volume	Percentage or transaction volume metric		
	7	Regulated entity deals with Debit, Credit Cards, Prepaid Cards or Person-to-Person Payments.	Use drop down list	- Does not provide card facilities. - Debit cards are issued using on premises solution. - Debit, Prepaid and credit cards are issued using on premise solution supported by employees / third party; and / or Number of Active Card Customers <100000. - Debit, Prepaid and credit cards are issued using on premise / third party hosted solution and supported by employees / third party; and / or Number of Active Card Customers <100000-500000. - Debit, Prepaid, Credit Cards and Person to Person payments are enabled using on premise / third party hosted solution and supported by employees /	

Tiering Dimension	#	Assessment Criteria	Guidance for Updating Values in the Adjacent Columns	Input to be Provided by the Regulated Entity	Comments -if any- from the Regulated Entity
				third party and / or Number of Active Card Customers >500000.	

Tiering Dimension	#	Assessment Criteria	Guidance for Updating Values in the Adjacent Columns	Input to be Provided by the Regulated Entity	Comments -if any- from the Regulated Entity
	8	Regulated entity works as a merchant acquirer.	Use drop down list	- Does not provide these services. - Dependent on other regulated entities / third parties for transaction acquisition. - Acts as a merchant acquirer; and / or Handles daily transactions to the tune of <10000. - Acts as a merchant acquirer; and / or act as a card payment processor for other entities; and /or Handles daily transactions to the tune of 10001 - 50000. - Acts as a merchant acquirer; and / or act as a card payment processor for other entities; and /or Handles daily transactions to the tune of >50000.	

Tiering Dimension	#	Assessment Criteria	Guidance for Updating Values in the Adjacent Columns	Input to be Provided by the Regulated Entity	Comments -if any- from the Regulated Entity
	9	Usage of contactless technology by customers of the Regulated entity.	Use drop down list	- Contactless technology not used. - Contactless technology use in nascent stage; and/or only limited volume domestic transactions using contactless technology: <20,000 per month. - Limited use of contactless technology; and/or only low volume domestic transactions using contactless technology: 20,000-50,000 per month. - Contactless technology used moderately; and/or moderate volume of transactions and foreign payments using contactless technology: 50,000-100000 per month. - Contactless technology used extensively; and/or high volume of transactions and foreign payments using contactless technology: >100000.	
Branch Network and Channels	10	Number of physical branches operating in Kuwait and how many abroad.	Two numeric values shall be provided		
	11	Number of ATM and ITM machines in Kuwait	Numeric value		

Tiering Dimension	#	Assessment Criteria	Guidance for Updating Values in the Adjacent Columns	Input to be Provided by the Regulated Entity	Comments -if any- from the Regulated Entity
	12	Do you operate a neobank (i.e., digital bank) brand?	Yes/No	- Yes - No	
	13	Online presence of the Regulated entity: Number of public facing Web and Mobile Applications.	Permitted values 0 to 100		
	14	Online presence of the Regulated entity: Number of Social Media Channels on which the entity has official presence.	Permitted Value 0-10 Answer this question only if there are official social media accounts of your entity.		
Customer Base	15	Total number of Unique Customers in GCC and Middle East Countries.	Permitted values 1 to 10000000		

Tiering Dimension	#	Assessment Criteria	Guidance for Updating Values in the Adjacent Columns	Input to be Provided by the Regulated Entity	Comments -if any- from the Regulated Entity
	16	Percentage of cross-boarder records of customers and employees from region where data protection and privacy laws exist.	Use drop down list	- < 2 % of Total Records. - 3-5 % of Total Records. - 5-10 % of Total Records. - 11-15 % of Total Records. - >15 % of Total Records.	
	17	Proportion of your retail customers versus corporate customers.	Percentage and descriptive split		
	18	Do you serve any large corporates or high-volume clients (e.g., government, large enterprises)? If yes, how many?	Yes/No; if yes, numeric value		
Nature and Breadth of Services	19	Type of services you provide (Select all that apply)	Use multiple-selection list	- Retail Banking. - Corporate Banking. - Investment/Wealth Management. - Financing/Lending. - Payment and/or Remittance Services. - Other - Specify.	
	20	Do you process cross-boarder payments or remittances?	Yes/No	- Yes - No	

Tiering Dimension	#	Assessment Criteria	Guidance for Updating Values in the Adjacent Columns	Input to be Provided by the Regulated Entity	Comments -if any- from the Regulated Entity
	21	Type of online services provided by Regulated entity.	Use drop down list	- No online services provided. - Web based online service provided. - Web based online services provided along with ATM and / or Point of Sale services. - Web and mobile based services provided along with ATM and / or Point of Sale services. - Web and mobile and contact services provided along with ATM and / or Point of Sale services.	
	22	Internet-based services provided by Regulated Entity.	Use drop down list	- Online banking is not enabled for customers. - Only static web pages and informational web pages or social media pages are hosted. - Online banking application supports retail banking and / or Number of services permitted: < 16. - Online banking application supports retail and wholesale banking transactions and / or Number of services permitted: 16-30. - Online banking application supports retail,	

Tiering Dimension	#	Assessment Criteria	Guidance for Updating Values in the Adjacent Columns	Input to be Provided by the Regulated Entity	Comments -if any- from the Regulated Entity
				wholesale and other allied services and / or Number of services permitted: > 30.	
	23	Mobile-based services provided by the Regulated Entity.	Use drop down list	- No mobile banking services. - SMS text alert and browser based Mobile access is enabled. - Mobile application is available for retail customers. Customers are allowed to make small value fund transfers, etc., Overall services enabled through mobile banking are <15. - Mobile application is available for retail customers.	

Tiering Dimension	#	Assessment Criteria	Guidance for Updating Values in the Adjacent Columns	Input to be Provided by the Regulated Entity	Comments -if any- from the Regulated Entity
				Customers are allowed to make small value fund transfers, etc., Overall services enabled through mobile banking are >15-30. - Mobile application is available for retail customers. Customers are allowed to register new payees, make high value funds transfers, etc., Overall services enabled through mobile banking are >30.	
	24	Are you required to comply with any of the following regulations due to nature of operations: 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	Use drop down list. Please specify the ones that you need to comply in the comments column	- Payment Cards Industry Data Security Standard (PCI-DSS); - Payment Application Data Security Standard (PA-DSS); - EMV (Europay, MasterCard, and VISA) technical standard; - SWIFT Customer Security Controls Framework - ISO 27001, 22301, 31000; and - GDPR or any other Privacy Regulations.	

Tiering Dimension	#	Assessment Criteria	Guidance for Updating Values in the Adjacent Columns	Input to be Provided by the Regulated Entity	Comments -if any- from the Regulated Entity
		Framework e) ISO 27001, 22301, 31000; and f) GDPR or any other Privacy Regulations.			
Infrastructure Role	25	Designated as Financial Market Infrastructure (FMI)	Yes/No **[This is to be answered by CBK Supervision Department]**	- Yes - No	
	26	Do you operate payment or settlement platforms used by other Regulated Entities?	Yes/No	- Yes - No	
	27	Do other entities depend on your platform for critical operations that cannot be substituted (e.g., credit information reporting, payment clearing, settlement)?	Yes/No	- Yes - No	
	28	Percentage of national payment or securities transactions your platform process, by volume or value.	Percentage		

Tiering Dimension	#	Assessment Criteria	Guidance for Updating Values in the Adjacent Columns	Input to be Provided by the Regulated Entity	Comments -if any- from the Regulated Entity
	29	Do you operate credit information or data sharing systems used by multiple entities?	Yes/No; if yes, specify	- Yes - No	
	30	Do you provide cross-boarder clearing or settlement services?	Yes/No; if yes, specify the nature of the cross-boarder services.	- Yes - No	
Technological Complexity	31	New products launch, adoption of new technologies during the last two years.	Use drop down list	- No new product or service launched - No emerging technologies were implemented during the last two years - No services were sunset during the last two years - New products were launched using existing technology - No emerging technologies were implemented during the last two years - No services were sunset during the last 2 years - New products were launched using existing technology however new development was required to customize existing solutions	

Tiering Dimension	#	Assessment Criteria	Guidance for Updating Values in the Adjacent Columns	Input to be Provided by the Regulated Entity	Comments -if any- from the Regulated Entity
				- No emerging technologies were implemented during the last two years - No services were sunset during the last 2 years - New products were launched using existing technology and existing solution required major updates - < 2 new emerging technologies were implemented during the last two years - At-least 2 services were sunset during the last 2 years - New products were launched using established technologies - > 3 new emerging technologies were implemented during the last two years - More than 2 services were sunset during the last two years.	

Tiering Dimension	#	Assessment Criteria	Guidance for Updating Values in the Adjacent Columns	Input to be Provided by the Regulated Entity	Comments -if any- from the Regulated Entity
	32	Type of cloud service used and type of data processed by regulated entity on cloud.	Use drop down list	- Cloud computing not used. - Only private cloud in use. - Public / private cloud computing services providers: 1-4; and/or Only data internal to the regulated entity processed on cloud. - Public / hybrid / private cloud computing services providers; 5-8; and/or Internal and customer data processed on cloud. - Public / hybrid / private / international cloud computing services providers: >8; and/or Internal and customer data processed on cloud.	
	33	Do you provide public APIs (Open banking interfaces) to third-parties?	Yes/No	- Yes - No	
	34	Do you use any type of AI/ML for credit scoring, fraud detection, or any other core functions?	Yes/No	- Yes - No	
	35	Percentage of your applications or workloads deployed on public/hybrid cloud	Percentage		

Tiering Dimension	#	Assessment Criteria	Guidance for Updating Values in the Adjacent Columns	Input to be Provided by the Regulated Entity	Comments -if any- from the Regulated Entity
Outsourcing and Third-Party Dependencies	36	Number of in-house developed applications.	Permitted values 0 to 500		
	37	Percentage of applications for which source code is available with the Regulated entity.	Use drop down list	- >80 % - 61% to 80% - 41% to 60% - 21% to 40% - Less than 20%	
	38	Percentage of IT Administrative support which is outsourced to third parties by the Regulated entity.	Use drop down list	- All administrators (privileged access) are managed by internal employees - <25% administrative roles (privileged access) are outsourced to third parties - 26-50% administrative roles (privileged access) are outsourced to third parties - 51-75% administrative roles (privileged access) are outsourced to third parties - >75% administrative roles (privileged access) are outsourced to third parties	

Tiering Dimension	#	Assessment Criteria	Guidance for Updating Values in the Adjacent Columns	Input to be Provided by the Regulated Entity	Comments -if any- from the Regulated Entity
	39	Usage of Open Source Software's (OSS).	Use drop down list	- No Open Source Software (OSS) - OSS exist however supports internal non-critical processes. - OSS exist however supports internal critical and non-critical processes. - OSS exist and supports most of the internal processes and / or support <5 customer facing processes. - OSS exist and supports most of the internal processes and / or support >5 customer facing processes.	
	40	Number of third party entities supporting Critical activities / applications.	Permitted values 0 to 20		
	41	Number of third party staff who has access to technology's assets.	Permitted valued 0 to 5000		

Tiering Dimension	#	Assessment Criteria	Guidance for Updating Values in the Adjacent Columns	Input to be Provided by the Regulated Entity	Comments -if any- from the Regulated Entity
	42	ATM Network Complexity.	Use drop down list	- No ATM services offered. - ATM services offered using its in house team and to own customers only. - ATM services are managed by in house team; and/ or cash reload services outsourced. - ATM services are managed by third party; and/ or are connected with other regulated entity payment systems; and/or cash reload services outsourced. - ATM services are managed by third party; and/ or are connected with other regulated entity payment systems; and/or cash reload services outsourced;	

Tiering Dimension	#	Assessment Criteria	Guidance for Updating Values in the Adjacent Columns	Input to be Provided by the Regulated Entity	Comments -if any- from the Regulated Entity
				and/ or connected to the internet.	
	43	Do you rely on third-party or vendor-hosted core banking platforms?	Yes/No	- Yes - No	
Cyber Risk Exposure and Threat Landscape	44	Number of Connections (Internet Service Provider Links, and Number of branch connectivity's provided other than through wireline MPLS).	Permitted values 1 to 1000		

Tiering Dimension	#	Assessment Criteria	Guidance for Updating Values in the Adjacent Columns	Input to be Provided by the Regulated Entity	Comments -if any- from the Regulated Entity
	45	Number of unsecured (other than end user VPN access) external connections (e.g., file transfer protocol [FTP], Telnet, remote login, other unsecured connections, etc.,).	Permitted values 1 to 1500		
	46	Details of Wireless Setup and Wireless Access within the entity.	Use drop down list	- No provision for wireless access - Physically segregated access points for guests and internal wireless users and there is no commingling of guests and Regulated entity data - Guest and internal wireless user network access points are logically segregated. Guest access is permitted post approval and on authorized device - Guest and internal wireless user network access points are logically separated. Guest access is permitted without approval - Guest and internal wireless user network access points are logically separated. Guest access is permitted without approval;	

Tiering Dimension	#	Assessment Criteria	Guidance for Updating Values in the Adjacent Columns	Input to be Provided by the Regulated Entity	Comments -if any- from the Regulated Entity
	46.A	A. Number of Wireless Users.	Permitted values 0 to 50000		
	46.B	B. Number of Access Points.	Permitted values 0 to 500		
	47	Percentage of application using encrypted URL's.	Use drop down list	- Applications communicating over HTTPS: >75% - Applications communicating over HTTPS: >50% - Applications communicating over HTTPS: >25% - Applications communicating over HTTPS: >10% - Applications communicating over HTTPS: <10%;	
	48	Number of changes in the IT Environment that required interruption of IT services for more than 1 hour during the last one year.	Permitted values 1 to 50		

Tiering Dimension	#	Assessment Criteria	Guidance for Updating Values in the Adjacent Columns	Input to be Provided by the Regulated Entity	Comments -if any- from the Regulated Entity
	49	Configuration and access to corporate email service.	Use drop down list	- Mail access provided to employees on need basis. - Mail client configured on end user system and no web mail access exist. - Mail access provided to employees and contractors by default on end user system; and / or Web mail access provided to select few. - Mail access provided to employees and contractors by default on end user system; and / or Mail access provided to employees through web post specific approvals for employees. - Mail access provided to employees and contractors by default on end user system; and / or Mail access provided to employees through web and do not need approvals. - Mail access provided to employees and	

Tiering Dimension	#	Assessment Criteria	Guidance for Updating Values in the Adjacent Columns	Input to be Provided by the Regulated Entity	Comments -if any- from the Regulated Entity
				contractors by default on end user system; and / or Mail access provided to employees and contractors through web do not need approvals.	

Tiering Dimension	#	Assessment Criteria	Guidance for Updating Values in the Adjacent Columns	Input to be Provided by the Regulated Entity	Comments -if any- from the Regulated Entity
	50	Employees and third-party staff are allowed to connect devices owned by them to Regulated entities Network.	Use drop down list	- No personal device allowed to connect to the corporate network - Only certain types of personal devices allowed to connect to the network - Multiple types of personal devices allowed to connect to the network - Multiple types of personal devices allowed to connect to the network; and employees can access internal email using such devices - Employees and Third Party staff are allowed to connect devices to the network and access internal email and applications using such devices	
	51	Percentage of employees and third-party staff allowed to connect devices owned by them to Regulated entities Network.	Use drop down list	- <5% of employees and third party staff use own devices - 5-15% of employees and third party staff use own devices - 16-35% of employees and third party staff use own	

Tiering Dimension	#	Assessment Criteria	Guidance for Updating Values in the Adjacent Columns	Input to be Provided by the Regulated Entity	Comments -if any- from the Regulated Entity
				devices - 36-50% of employees and third party staff use own devices - >50% of employees and third party staff use own devices.	
	52	Number of security incidents / attempted attacks (External Threat Attacks) or reconnaissance on the Technology Assets during the last one year.	Permitted values 0 to 100		
	53	Number of data or security breaches during the last one year.	Permitted values 0 to 100		
	54	Malware attacks.	Use drop down list	- Malware impacted few end points during the last year. - Malware were detected on data center assets such as servers, databases, middleware, etc. - Malware impacted data center assets such as servers, databases, middleware, etc. - Malware impacted data center assets such as	

Tiering Dimension	#	Assessment Criteria	Guidance for Updating Values in the Adjacent Columns	Input to be Provided by the Regulated Entity	Comments -if any- from the Regulated Entity
				servers, databases, middleware, etc., supporting critical applications. - Malware impacted data center assets such as servers, databases, middleware, etc., supporting critical applications leading to wide scale outage.	
	55	Attempts for social engineering (Phishing, Vishing, SMShing, Social engineering incidents).	Use drop down list	- No reported social engineering incident - Few employees have been target of social engineering attacks. - Employees and customers have been target of social engineering attacks. - Employees and customers have been target of customized social engineering attacks. - Senior management have been target of social engineering attacks.	
	56	Distributed Denial of Service (DDoS) attempts detected per year.	Permitted values 1 to 100		

Tiering Dimension	#	Assessment Criteria	Guidance for Updating Values in the Adjacent Columns	Input to be Provided by the Regulated Entity	Comments -if any- from the Regulated Entity
	57	Number of solutions (Applications, Operating Systems, Databases, Middleware, Security Devices) that are already or will reach End of Life (EOL) within one year.	Permitted values 0 to 50	- No solutions are / will be EOL within one year. - Number of Solutions that are / will be EOL within one year: 1. - Number of Solutions that are / will be EOL within one year: 2-3. - Number of Solutions that are / will be EOL within one year: 4-5. - Number of Solutions that are / will be EOL within one year: >5.	
	58	Data Centre and Disaster Recovery site readiness.	Use drop down list	- Data Centre and Disaster Recovery sites are at least 80 Kms apart. - Data Centre and Disaster Recovery Sites are at least 50 Kms apart; and / or No outage has happened during the last 2 years due to environmental issues. - Data Centre and Disaster Recovery sites are 11-49 km away;	

Tiering Dimension	#	Assessment Criteria	Guidance for Updating Values in the Adjacent Columns	Input to be Provided by the Regulated Entity	Comments -if any- from the Regulated Entity
				And / or Minor outage has happened in the data center due to environmental issues during the last 2 years. - Data Centre and Disaster Recovery sites 1-10 km away; And / or Major outage has happened in the data center due to environmental issues during the last 2 years. - Data Centre and Disaster Recovery sites are in same premises or < 1 km away; And / or Major outage has happened in the data center due to environmental issues during the last 1 year.	
Regulatory and Supervisory History	59	Regulatory penalties, sanctions, or directives received related to cyber and information security or operational resilience in the past three years	Yes/No	- Yes - No	

Tiering Dimension	#	Assessment Criteria	Guidance for Updating Values in the Adjacent Columns	Input to be Provided by the Regulated Entity	Comments -if any- from the Regulated Entity
	60	Number of material findings reported in the last CBK cyber and information security or resilience assessment, audit, and/or inspection.	Numeric value **[This is to be provided by CBK]**		
	61	Whether independent cybersecurity audits were performed by internal audit or independent entities during the last year.	Use drop down list	- Independent cybersecurity audits were performed by independent entities and internal audit has covered all areas from the baseline document as part of the yearly testing; - No cybersecurity assessments were performed by independent entities during the year. 21 to 30 sub domains from the baseline documents were covered in the thematic audits performed by the internal audit team during last one year. - No cybersecurity assessments were performed by independent entities during the year. 10 - 20 sub domains from the baseline documents were covered in the thematic audits performed by the internal audit team during last one year;	

Tiering Dimension	#	Assessment Criteria	Guidance for Updating Values in the Adjacent Columns	Input to be Provided by the Regulated Entity	Comments -if any- from the Regulated Entity
				- No cybersecurity assessments were performed by independent during the year. Less than 9 sub domains from the baseline documents were covered in the thematic audits performed by the internal audit team during last one year; - No cybersecurity assessments were performed by independent entities or internal audit teams during the year;	
	62	The location from where Management and Board Operates.	Use drop down list	- Board and Senior management operates from Kuwait - Senior management operates from Kuwait - Senior management and Board operates from outside of Kuwait	

Tiering Dimension	#	Assessment Criteria	Guidance for Updating Values in the Adjacent Columns	Input to be Provided by the Regulated Entity	Comments -if any- from the Regulated Entity
Cyber Resilience Workforce	63	Total Number of Employee and Third Party Contractors Operating within GCC and Middle East Countries.	Permitted values between 1 to 100000		
	64	Size of team involved in information technology and cybersecurity activities (including third party staff) in GCC and Middle East Countries.	Permitted values between 1 to 10000		
	65	Number of key and senior personnel from IT and Cyber Security who have left the entity in last 12 months.	Permitted values 0 to 10	- No turnover of key and senior personnel. - Turnover of key and senior personnel 1-2 people in last 12 months. - Turnover of key and senior personnel 3-4 people in last 12 months. - Turnover of key and senior personnel 5-6 people in last 12 months. - Turnover of key and senior personnel > 6 people in last 12 months.	

Tiering Dimension	#	Assessment Criteria	Guidance for Updating Values in the Adjacent Columns	Input to be Provided by the Regulated Entity	Comments -if any- from the Regulated Entity
	66	Number of vacancies in 'Key Positions' in IT and Cybersecurity Team.	Use drop down list	- Key IT and Security positions are filled. - Non critical staff vacancies exist in IT and Security Team for less than 3 month. - Non critical staff vacancies exist in IT and Security Team for over 3 months. - Critical staff vacancies exist in IT and Security Team for less than 3 months. - Critical staff vacancies exist in IT and Security Team for over 3 months.	
	67	You have a formally designated CISO or equivalent role.	Yes/No; if yes, specify to whom does the CISO report.	- Yes - No	
	68	Percentage of cyber and information security team members holding industry-recognized certifications (e.g., ISO 27001 LI/LA, CISM, CISSP, CISM).	Use drop down list	- Less than 10% - 10% - 25% - 26% - 50% - 51% - 75% - More than 75%	

8.3 CORF Assessment Report Template

CORF Evaluation Report	
Regulated Entity Name	
Regulated Entity Assessor	
Baselines	Cyber Resilience Baselines | OR Baselines | TPRM Baselines
Assessment Year	

Overall Average Maturity Score		Overall Compliance Percentage	

Cyber Resilience Baselines |OR Baselines | TPRM Baselines Domain Overview

Cyber Resilience Baselines					
Domain	*Governance, Risk, and Compliance*	Compliance Percentage	*X%*	Average Maturity	*Level X*
Domain	*Technology and Operations*	Compliance Percentage	*X%*	Average Maturity	*Level X*
Domain	*Emerging Technologies*	Compliance Percentage	*X%*	Average Maturity	*Level X*
Domain	*Third-Party Risk Management and Supply Chain Management*	Compliance Percentage	*X%*	Average Maturity	*Level X*
Domain	*Governance, Risk, and Compliance*	Compliance Percentage	*X%*	Average Maturity	*Level X*

Operational Resilience Baselines					
Domain	*Governance and Oversight*	Compliance Percentage	*X%*	Average Maturity	*Level X*
Domain	*Risk and Threat Management*	Compliance Percentage	*X%*	Average Maturity	*Level X*
Domain	*Business Continuity Management*	Compliance Percentage	*X%*	Average Maturity	*Level X*
Domain	*Technology Resilience*	Compliance Percentage	*X%*	Average Maturity	*Level X*
Domain	*Third-Party Resilience*	Compliance Percentage	*X%*	Average Maturity	*Level X*
Domain	*Incident and Crisis Management*	Compliance Percentage	*X%*	Average Maturity	*Level X*
Domain	*Cyber Resilience*	Compliance Percentage	*X%*	Average Maturity	*Level X*
Domain	*Testing, Training, and Continuous Improvement*	Compliance Percentage	*X%*	Average Maturity	*Level X*

TPRM Baselines					
Domain	*Governance Structure and Oversight*	Compliance Percentage	*X%*	Average Maturity	*Level X*
Domain	*Risk Management Framework*	Compliance Percentage	*X%*	Average Maturity	*Level X*
Domain	*Contractual Agreements Considerations*	Compliance Percentage	*X%*	Average Maturity	*Level X*
Domain	*Risk Assessment and Monitoring*	Compliance Percentage	*X%*	Average Maturity	*Level X*
Domain	*Business Continuity Management and Disaster Recovery*	Compliance Percentage	*X%*	Average Maturity	*Level X*
Domain	*Incident Management*	Compliance Percentage	*X%*	Average Maturity	*Level X*
Domain	*Data Protection and Confidentiality*	Compliance Percentage	*X%*	Average Maturity	*Level X*

Domain	*Sub-Contracting*	Compliance Percentage	*X%*	Average Maturity	*Level X*
Domain	*Exit Strategy*	Compliance Percentage	*X%*	Average Maturity	*Level X*
Domain	*Storage of Data*	Compliance Percentage	*X%*	Average Maturity	*Level X*
Domain	*Cross-Border Transaction*	Compliance Percentage	*X%*	Average Maturity	*Level X*
Domain	*Usage of Cloud Services*	Compliance Percentage	*X%*	Average Maturity	*Level X*
Domain	*Inter-Affiliates*	Compliance Percentage	*X%*	Average Maturity	*Level X*

Detailed Assessment Report					
Domain	*Domain 1*	Compliance Percentage	*X%*	Average Maturity	*Level X*
Subdomain	*Subdomain 1*	Compliance Percentage	*X%*	Maturity Rating	*Level X*
Maturity Rationale		**Areas of Improvement**			

8.4 Exemptions to the CORF Template

CORF Exemption Request

Regulated Entity Name	
Baselines	Cyber Resilience Baselines | OR Baselines | TPRM Baselines
Date of Submission	
Reference Number	

Requested Exemption Details							
Domain	**Sub-Domain**	**Control Area**	**Control ID**	**Control Statement**	**Exemption Duration (Permanent/ Temporary)**	**Description of the Requested Exemption**	**Justification of the Request (e.g., Technical, Legal, Operational, Business Reasons)**

Risk Assessment			
Summary of Risks		**Potential Impact on Services, Operations, Customers, or Compliance**	
Affected Services/Assets		**Risk Rating**	
Compensating Controls		**Implementation Timeline for Compensating Controls**	
Requested Duration of Exemption			

Approvals	
Regulated Entity Reviewer	
Regulated Entity Approver	
CBK Reviewer	
CBK Approver	
CBK Comments	

9. Circulars

10.Appendices

10.1 Appendix A – Cyber Resilience Baselines

This appendix presents the maturity attributes across each sub-domain of the CBK Cyber Resilience Baselines

Domain – Governance, Risk and Compliance				
Sub-Domain – Cybersecurity Governance and Oversight				
Level 1 – Initial	**Level 2 – Ad-hoc**	**Level 3 – Baseline**	**Level 4 – Advanced**	**Level 5 – Innovative**
▪ No formal cybersecurity governance structure is in place. ▪ The Board, or equivalent, and the Executive/Senior Management are not actively engaged in cybersecurity oversight. ▪ Cybersecurity roles and responsibilities are undefined or unclear. ▪ There is no documented cybersecurity strategy or policy. ▪ The Information Security function is either non-existent or embedded within IT with no independent authority.	▪ Some awareness exists at the Board, or equivalent, and the Executive/Senior Management level, but engagement is inconsistent. ▪ A cybersecurity strategy or policy exist, but is generic, outdated, or not approved at the appropriate level. ▪ The Information Security function exists but lacks independence and formal empowerment. ▪ A Cybersecurity Steering Committee is in place but operates without a	▪ A formal cybersecurity strategy and policy are defined, aligned with regulatory and business requirements, approved, communicated, and reviewed at least annually. ▪ The Board, or equivalent, approves the cybersecurity strategy and provides attestation or authorization of the cybersecurity policy. ▪ The Cybersecurity Steering Committee is formally established with a documented charter, meets	▪ Cybersecurity strategy is formally aligned with the enterprise strategy. ▪ Cybersecurity governance is systematically managed and automated, with governance processes embedded into the entity's centralized platform (e.g. GRC platform). ▪ A centralized platform (e.g., GRC platform) is used for managing cybersecurity policy full lifecycle, including development, review, approval, publication, and version control,	▪ The Entity leverages AI/ML and data analytics to enhance decision-making and strategic oversight to achieve an intelligence-driven, predictive, and continuously optimized cybersecurity governance. ▪ The centralized platform (e.g. GRC platform) is supported with AI-enabled features that provide real-time insights, flag governance anomalies, and recommend corrective actions (e.g., identifying delayed approvals, policy

Domain – Governance, Risk and Compliance				
Sub-Domain – Cybersecurity Governance and Oversight				
Level 1 – Initial	**Level 2 – Ad-hoc**	**Level 3 – Baseline**	**Level 4 – Advanced**	**Level 5 – Innovative**
	formal charter or frequent meetings. ▪ Cybersecurity roles and responsibilities are defined but are not fully aligned or documented across functions.	quarterly, and chaired by a qualified senior executive with the relevant knowledge and skills. ▪ Executive/Senior Management ensures execution of the approved strategy, allocation of adequate resources, and oversight of policy implementation. ▪ Information Security function is independent from IT Operations, appropriately staffed, and have the authority to oversee cybersecurity activities. ▪ Clear cybersecurity roles and responsibilities, with clear accountability are defined. ▪ Regular reporting is provided to the Board, or equivalent, on cybersecurity status, risks, and emerging threats.	ensuring consistency, traceability, and alignment with legal and regulatory requirements. ▪ Approvals, delegations, and decision-making processes are tracked through automated workflows.	misalignments, or gaps in risk tolerance). ▪ Predictive analytics are used to anticipate governance risks, such as emerging threats, resource deficiencies, or regulatory shifts, enabling proactive adjustments to governance structures and strategies. ▪ The Board, Cybersecurity Steering Committee, and Executive/Senior Management are equipped with interactive and real-time dashboards offering visibility into cyber risk exposure, policy performance, and the effectiveness of governance controls.

Domain – Governance, Risk and Compliance				
Sub-Domain – Cybersecurity Risk Management				
Level 1 – Initial	**Level 2 – Ad-hoc**	**Level 3 – Baseline**	**Level 4 – Advanced**	**Level 5 – Innovative**
▪ There is no defined or documented cybersecurity risk management methodology. ▪ Cybersecurity risk management activities are reactive, informal, and performed without structure or coordination. ▪ Cyber risk assessments – if any- are sporadic/infrequent and undocumented. ▪ Roles and responsibilities for cybersecurity risks are not defined across business or technology teams. ▪ Risks are not identified, recorded, or tracked in a structured way; no centralized risk register exists. ▪ Cyber risk appetite and tolerance levels are not defined.	▪ A basic cybersecurity risk management approach exists, but it is informally practiced, undocumented, inconsistently applied, or not formally approved by Executive/Senior Management. ▪ Cyber risk assessments are performed on an ad-hoc basis, typically driven by audits, incidents, or regulatory triggers. ▪ Documentation of risks and controls exists, but incomplete, inaccurate, or inconsistent. ▪ Cybersecurity risks are tracked separately (e.g., disconnected spreadsheets/systems or informal formats); no centralized or consistently updated risk register. ▪ Risk and controls ownership is	▪ A formal, documented, and approved cybersecurity risk management methodology is implemented and aligned with industry standards and best practices. ▪ The methodology clearly outlines the scope, frequency, roles and responsibilities, and execution of cybersecurity risk assessments. ▪ Cybersecurity risk assessments are conducted at least annually or whenever triggered by defined change or threat scenarios. ▪ A centralized cybersecurity risk register is maintained, capturing risks, threats, vulnerabilities, controls, assets,	▪ Cybersecurity risk management is fully integrated across the Entity and aligned with the Entity's overall Enterprise Risk Management (ERM) framework. ▪ Emerging threats are proactively monitored using structured threat intelligence feeds, industry reports, and cyber risk insights. ▪ Control effectiveness is continuously measured and monitored, with periodic testing and performance reviews (at least quarterly). ▪ An Integrated Risk Management (IRM)/ Governance Risk Compliance (GRC) platform is in place to manage the entire cybersecurity risk lifecycle, with	▪ Cybersecurity risk management is predictive, data-driven, and tightly integrated with enterprise governance (i.e., actively supports strategic and transformation initiatives across the Entity.) ▪ The Entity utilizes advanced technologies (e.g., AI/ML) to support real-time risk correlation, anomaly detection, predictive modeling, and prioritizing of emerging threats. ▪ Quantitative methods (e.g., Factor Analysis of Information Risk (FAIR), Monte Carlo) and scenario-based modeling are applied to estimate potential impact and guide

Domain – Governance, Risk and Compliance				
Sub-Domain – Cybersecurity Risk Management				
Level 1 – Initial	**Level 2 – Ad-hoc**	**Level 3 – Baseline**	**Level 4 – Advanced**	**Level 5 – Innovative**
▪ Cybersecurity considerations are not factored into projects or business decisions. ▪ There is no assignment of risk or control ownership; no accountability framework exists. ▪ Control effectiveness is not assessed or monitored. ▪ Threats and vulnerabilities are not systematically identified or analyzed.	inconsistently defined or applied across the Entity. ▪ Cybersecurity risks are sometimes considered during projects, but inconsistently, not in early phases of the project lifecycle, or there is no formal integration into the lifecycle. ▪ Risk treatment is inconsistently tracked; decisions are not formally categorized, justified, or approved. ▪ Threats are recognized/identified reactively; there is no structured threat intelligence or proactive monitoring process. ▪ Risk appetite and tolerance are vague and/or are not applied to guide decisions. ▪ Some awareness exists among stakeholders, but communication is irregular.	relevant scores and ratings, residual risks, and treatment strategies. ▪ Risk and control ownership are formally assigned and documented across relevant business and technology teams. ▪ Cybersecurity risk appetite and tolerance levels are defined in alignment with enterprise-wide strategy and integrated into risk analysis and treatment. ▪ Risk treatment plans are categorized, documented, justified, tracked and monitored for completion. ▪ Cybersecurity considerations are formally integrated into project, procurement, and third-party risk management processes, using	utilization of capabilities for risk scoring, workflow-based treatment tracking, and automated alerts or escalations based on predefined timeline or severity thresholds.	strategic treatment decisions. ▪ The Entity integrates live threat intelligence feeds into its risk posture and treatment activities, enabling continuous alignment with current risks (dynamic risk profiling and treatment adjustments). ▪ Cyber risk appetite and tolerance levels are adaptive and reviewed in sync with evolving business needs and priorities. ▪ Controls effectiveness is validated continuously using adversarial simulations, red teaming, and other advanced exercises. ▪ Executive dashboards provide real-time visibility into cybersecurity risk posture, treatment progress, and control

Domain – Governance, Risk and Compliance				
Sub-Domain – Cybersecurity Risk Management				
Level 1 – Initial	**Level 2 – Ad-hoc**	**Level 3 – Baseline**	**Level 4 – Advanced**	**Level 5 – Innovative**
		standardized templates and checkpoints. ▪ Communication and awareness of the methodology are conducted annually, reaching all relevant functions. ▪ Control effectiveness is considered during risk treatment planning, although continuous monitoring may be limited.		performance (through the IRM/GRC platform). ▪ Cyber insurance policy is regularly reviewed, strategically managed and optimized, considering evolving threats, exclusions, and financial exposure (ROI analysis and active claims monitoring).

Domain – Governance, Risk and Compliance				
Sub-Domain – Compliance				
Level 1 – Initial	**Level 2 – Ad-hoc**	**Level 3 – Baseline**	**Level 4 – Advanced**	**Level 5 – Innovative**
▪ Regulatory and legal compliance requirements are not consistently identified or documented. ▪ Compliance activities are reactive, conducted only when triggered by audits or incidents. ▪ There is no formal compliance register.	▪ Compliance requirements are partially identified and informally tracked. ▪ Some standards are acknowledged, but compliance is inconsistent. ▪ A basic compliance register exists but is not updated regularly.	▪ All applicable legal and regulatory requirements are identified, documented, and demonstrably complied with. ▪ Compliance with industry standards is fully achieved, and required certifications and attestations are maintained.	▪ Compliance management is centralized and technology-enabled (e.g., using GRC solutions) solution. ▪ Processes for monitoring changes in regulatory compliance are automated (e.g., alerts and notifications).	▪ AI-powered tools are used to continuously scan regulatory sources to detect and identify any new or updated requirements. ▪ AI/ML technologies are used to predict regulatory changes impact and recommend control adjustments.

Domain – Governance, Risk and Compliance				
Sub-Domain – Compliance				
Level 1 – Initial	**Level 2 – Ad-hoc**	**Level 3 – Baseline**	**Level 4 – Advanced**	**Level 5 – Innovative**
▪ None of the required certifications are actively achieved or maintained. ▪ Lack of awareness of national cybersecurity or sectoral compliance mandates.	▪ Certifications are in process, but not yet obtained or periodically renewed. ▪ Internal compliance processes are manual and fragmented across departments.	▪ A formal compliance register is in place, reviewed and updated regularly –at least annually-. ▪ Changes to legal and regulatory requirements are manually tracked and assessed, and corresponding updates are reflected in the compliance register. ▪ Compliance practices are repeatable, documented, and embedded into the entity's core operations.	▪ Compliance register is linked to risk registers and control libraries for unified GRC oversight at the enterprise level. ▪ Metrics are used to assess compliance posture and drive continuous improvements.	▪ RegTech solutions are leveraged for automated compliance mapping, impact workflows, evidence collection, reporting, and certification tracking processes. ▪ Real-time compliance monitoring with automated dashboards is utilized.

Domain – Governance, Risk, and Compliance				
Sub-Domain – Independent Audit				
Level 1 – Initial	**Level 2 – Ad-hoc**	**Level 3 – Baseline**	**Level 4 – Advanced**	**Level 5 – Innovative**
▪ No formal approved audit charter is in place. ▪ Cybersecurity is not specifically covered in audit activities. ▪ Audits, if conducted, are ad-hoc and not	▪ A basic audit charter exist but is not aligned with industry standards and cybersecurity frameworks, or is not approved by the Board, or equivalent, or	▪ An audit charter aligned with accepted audit standards and the Cyber Resilience Baselines is defined, approved, and reviewed annually.	▪ Cybersecurity audit activities are centrally managed and supported by centralized platform (e.g. a GRC solution), enabling risk-based audit planning,	▪ Advanced technologies, such as AI/ML and data analytics tools, are used to enhance the effectiveness, accuracy, and coverage of cybersecurity audits.

Domain – Governance, Risk, and Compliance				
Sub-Domain – Independent Audit				
Level 1 – Initial	**Level 2 – Ad-hoc**	**Level 3 – Baseline**	**Level 4 – Advanced**	**Level 5 – Innovative**
based on a defined plan or risk classification. ▪ No cybersecurity audits by independent third-parties are conducted. ▪ The cybersecurity audit results are not being reported to the Board, or equivalent, on periodic basis.	Executive/Senior Management. ▪ Cybersecurity audits are inconsistently planned and executed, with limited risk-based prioritization. ▪ Audits by independent third-parties are conducted, but not by CBK-approved auditors. ▪ Reporting on cybersecurity audit results to the Board, or equivalent, is irregular. ▪ Limited tracking and follow-ups on audit findings.	▪ A formal cybersecurity audit plan is in place and approved. ▪ Risk areas are classified using a defined methodology, and audit frequencies align with the Cyber Resilience Baselines requirements. ▪ Independent third-party audits are conducted by a CBK-approved and experienced auditors. ▪ Audit firms are changed/rotated at least once every two years. ▪ Audit results, including high-risk findings and corrective actions, are reported to the Board, or equivalent, on quarterly basis. ▪ A compliance dashboard is published to the Board, or equivalent, quarterly, tracking audit findings and remediation status.	execution, tracking of findings, and automated reporting. ▪ Audit findings are tracked through automated workflows that assign ownership, set deadlines, and escalate overdue items. ▪ Where additional tools are used for testing or analytics, these are integrated with the centralized platform (e.g. GRC platform) to ensure consistency across audit and risk management processes.	▪ AI/ML capabilities are leveraged to automate routine audit tasks, process and analyze large volumes of audit and control data, and identify any hidden patterns, anomalies, or indicators of potential fraud or non-compliance. ▪ Predictive analytics are used to anticipate control weaknesses and inform dynamic and risk-based adjustments to audit plans. ▪ Interactive dashboards to present real-time audit insights, covering audit status, remediation, and residual risks.

Domain – Governance, Risk and Compliance				
Sub-Domain – Workforce Management				
Level 1 – Initial	**Level 2 – Ad-hoc**	**Level 3 – Baseline**	**Level 4 – Advanced**	**Level 5 – Innovative**
▪ There is no defined or documented approach to cyber resilience workforce management. ▪ Personnel security measures, such as background checks and NDAs, are informal and inconsistently applied. ▪ Security awareness and training programs are non-existent or sporadic, lacking structure and coordination. ▪ Roles and responsibilities related to cyber resilience workforce management are not defined. ▪ There is no formal process for monitoring adherence to security policies or conducting disciplinary actions. ▪ Talent management strategies for cybersecurity roles are undefined, with no	▪ Basic personnel security measures exist but are informally practiced and inconsistently applied. ▪ Security awareness and training programs are conducted on an ad-hoc basis, often driven by incidents or regulatory requirements. ▪ Documentation of personnel security policies and training programs is incomplete or inconsistent. ▪ Adherence to security policies is tracked informally, with no centralized system for monitoring. ▪ Talent management strategies are inconsistently applied, with some roles lacking defined skill development plans. ▪ Specialist training for critical roles is occasionally provided	▪ A formal, documented approach to cyber resilience workforce management is implemented, aligned with industry standards. ▪ Personnel security measures, including background checks and NDAs, are standardized and consistently applied. ▪ Security awareness and training programs are formally established, with roles and responsibilities clearly defined. ▪ Talent management strategies include defined certification plans and skill development for critical roles. ▪ Specialist training for Board members and other critical roles is formally integrated into the training program.	▪ Cybersecurity workforce management is fully integrated across the Entity, aligned with overall HR and security strategies. ▪ Personnel security measures are proactively monitored, with regular updates to policies and practices. ▪ Security awareness and training programs are customized to roles and continuously updated based on emerging threats. ▪ A centralized system is in place to monitor adherence to security policies and conduct disciplinary actions ▪ An integrated platform is used to track adherence to security policies and manage disciplinary actions. ▪ Talent management strategies are dynamic, with continuous skill	▪ Cybersecurity workforce management is data-driven, actively supporting strategic initiatives. ▪ Advanced technologies are used to enhance personnel security measures, including real-time monitoring and anomaly detection. ▪ Security awareness and training programs utilize AI/ML to customize content and delivery based on individual roles and needs. ▪ A dynamic platform provides real-time visibility into adherence to security policies and workforce management practices. ▪ Talent management strategies are adaptive, with real-time updates to skill development plans based on evolving threats.

Domain – Governance, Risk and Compliance				
Sub-Domain – Workforce Management				
Level 1 – Initial	**Level 2 – Ad-hoc**	**Level 3 – Baseline**	**Level 4 – Advanced**	**Level 5 – Innovative**
certification or skill development plans. ▪ Specialist training for critical roles, including Board members, is not considered. ▪ Effectiveness of any existing training programs is not assessed or monitored.	but lacks formal structure. ▪ Communication regarding workforce management practices is irregular and informal.	▪ Effectiveness of training programs is assessed annually, with feedback mechanisms in place.	development plans for all cybersecurity roles. ▪ Specialist training is regularly updated and includes advanced topics relevant to critical roles. ▪ Training program effectiveness is continuously monitored, with periodic reviews and updates.	▪ Specialist training is integrated with live threat intelligence, ensuring continuous alignment with current risks. ▪ Executive dashboards provide real-time insights into workforce management effectiveness and training progress.

Domain – Technology & Operations				
Sub-Domain – Security Architecture Design				
Level 1 – Initial	**Level 2 – Ad-hoc**	**Level 3 – Baseline**	**Level 4 – Advanced**	**Level 5 – Innovative**
▪ Security architecture is not formally documented. ▪ Security architecture does not follow specific standards and best practices.	▪ Informal practices exist for security architecture design, but formal documentation is lacking. ▪ Security architecture design does not cover all systems and networks. ▪ Security architecture reviews are conducted on ad-hoc basis.	▪ Security architecture is formally documented, implemented and monitored across all systems and networks. ▪ Security architecture reviews are conducted annually and whenever changes to the environment or business requirements arise.	▪ Cybersecurity strategy has defined cybersecurity architecture and integrations in alignment with the overall business strategy. ▪ Security architecture processes are optimized based on industry best practices.	▪ Continuous process improvement and maturity modeling are used to optimize security architecture processes. ▪ Comprehensive AI models and machine learning are leveraged to optimize the assessment, and design of the entity's security architecture based on the defined principles.

Domain – Technology & Operations				
Sub-Domain – Security Architecture Design				
Level 1 – Initial	**Level 2 – Ad-hoc**	**Level 3 – Baseline**	**Level 4 – Advanced**	**Level 5 – Innovative**
		▪ Security architecture revies and updates are conducted based on business requirements taking into consideration risk and vulnerability assessments outcomes, cyber intelligence, best practices and cyber standards. ▪ Zero-trust architecture principles have been implemented across all environments, ensuring users, devices and applications are not trusted by default. ▪ Micro-segmentation design is implemented to isolate critical systems and data and reduce attack surface. ▪ Integration of Business Continuity and Disaster Recovery plans and processes with the cyber architecture designs.		▪ Additional features/facilities are incorporated / integrated for threat visibility

Domain – Technology & Operations				
Sub-Domain – Asset Management				
Level 1 – Initial	**Level 2 – Ad-hoc**	**Level 3 – Baseline**	**Level 4 – Advanced**	**Level 5 – Innovative**
▪ Asset management processes are ad hoc and not formally documented. ▪ There is no complete or centralized asset inventory. ▪ Asset discovery is conducted manually, outdated or tracked reactively with minimal oversight. ▪ Asset inventory records lack key metadata such as owner, custodian, classification and end of life/support information.	▪ Informal Asset management practices with minimal documentation. ▪ Some asset inventories exist with the focus on critical systems. ▪ Asset discovery is conducted on ad-hoc basis and does not cover the entire enterprise network. ▪ Asset tagging and classification are in consistent across business units. ▪ Maintenance and asset disposition activities informally logged.	▪ Formalized Asset management processes with documentation. ▪ Regular monitoring and reporting of Asset utilization and security. ▪ Established Asset management policies and frameworks. ▪ Defined roles and responsibilities for managing assets. ▪ Threat-informed adjustments begin, but full integration is lacking. ▪ Use of Asset management tools for tracking and reporting.	▪ Asset management processes are fully implemented and monitored using dashboards. ▪ Decisions are based on prior incidents, Threat intelligence, and risk assessments. ▪ Comprehensive Asset management framework with Regular updates. ▪ Automated alerts for Asset configuration Changes and anomalies. ▪ Continuous improvement and refinement of Asset management practices. ▪ Integration with other IT management systems for holistic oversight.	▪ Asset management processes are proactive, Automated, and data-driven. ▪ AI and real-time tools are used for optimization and predictive analysis. ▪ Continuous improvement is embedded in workflows and governance. ▪ Advanced analytics for Asset utilization and security metrics. ▪ Asset management is integrated with the overall risk management strategy. ▪ Use of Advanced technologies to discover IT/IoT in real-time for asset tracking and management.

Domain – Technology & Operations				
Sub-Domain – Infrastructure and Network Security				
Level 1 – Initial	**Level 2 – Ad-hoc**	**Level 3 – Baseline**	**Level 4 – Advanced**	**Level 5 – Innovative**
▪ Security configuration standards are not based on any global best practices or guidelines. ▪ Implementation of security configurations is inconsistent within the environment and conducted in a reactive mode. ▪ Lack of awareness of global best practices and guidelines. ▪ No structured approach to security configuration management. ▪ Network security architecture is not formally documented.	▪ Basic security configuration standards are defined, referencing some global best practices and guidelines. ▪ Internal policies are documented but not consistently followed. ▪ Implementation of security configurations follows basic guidelines but lacks consistency. ▪ Some awareness and training on global best practices and guidelines. ▪ Initial steps towards formalizing security configuration management. ▪ Basic network security controls in place. ▪ Network security controls are not hardened. ▪ Network security architecture is documented.	▪ Cybersecurity configuration standards are formally defined including but not limited to network security encryption, authentication, session management, session time-outs, access governance and data security. ▪ Cybersecurity configuration standards are aligned with national and international best practices, vendor guidelines and internal policies. ▪ Cybersecurity configurations are consistently implemented, approved, regularly monitored against security configuration standards across all technology assets. ▪ All new technology deployments are	▪ A formal risk-driven approach is defined for approving and implementing security configurations. ▪ Automated continuous Security configurations monitoring through a defined set of quantitatively measured metrics to ensure effectiveness and compliance. ▪ Standardized threat intelligence feeds, periodic threat analysis, basic integration of CTI with network security controls such as IDS/IPS, with regular updates to threat databases. ▪ Regular audits and assessments to ensure alignment with evolving threats and global best practices. ▪ Network security architecture is reviewed and updated based on post security incidents	▪ Comprehensive AI models and machine learning are leveraged to automate and optimize and adjustments security configuration settings. ▪ Advanced AI algorithms for continuous configuration optimization, automated detection and remediation of misconfigurations.

Domain – Technology & Operations				
Sub-Domain – Infrastructure and Network Security				
Level 1 – Initial	**Level 2 – Ad-hoc**	**Level 3 – Baseline**	**Level 4 – Advanced**	**Level 5 – Innovative**
		configured as per the configuration standards, and testing for compliance is performed prior to the production implementation. ▪ Network security architecture and data flows are formally defined and documented and updated whenever changes to the architecture take place. ▪ Network is segregated into production, testing, and development zones with distinct established network security policies for each zone, based on its criticality, purpose, and risk exposure. ▪ DMZs are implemented to host publicly accessible services, limiting inbound traffic to specific IPs, protocols, and ports.	reports learned lessons and recommendations. ▪ Network security micro-segmentation controls are implemented for reduced attack surface and improved breach containment. ▪ Deception technologies are implemented, continuously monitored.	

Domain – Technology & Operations				
Sub-Domain – Infrastructure and Network Security				
Level 1 – Initial	**Level 2 – Ad-hoc**	**Level 3 – Baseline**	**Level 4 – Advanced**	**Level 5 – Innovative**
		▪ Network is continuously monitored to detect unauthorized or rogue devices connected to the network. Any such devices are immediately isolated or deactivated upon detection. ▪ Zero trust architecture is implemented.		

Domain – Technology & Operations				
Sub-Domain – Endpoint and Device Security				
Level 1 – Initial	**Level 2 – Ad-hoc**	**Level 3 – Baseline**	**Level 4 – Advanced**	**Level 5 – Innovative**
▪ Endpoint and device security processes and policies are ad-hoc and undocumented. ▪ Endpoints and portable devices operate without any consistent security controls or hardening. ▪ Antivirus or security agents for endpoints and portable devices are missing, outdated, or disabled. ▪ No controls are in place to prevent unauthorized software	▪ Informal security practices for endpoints and portable devices with minimal documentation and some effort to follow best practices, but execution is inconsistent. ▪ Basic security policies for endpoints and portable devices exist but are not consistently enforced. ▪ Occasional reviews of Endpoint and portable	▪ Formalized Endpoint and portable device security processes and policies with documentation. ▪ Endpoint and portable device configurations are continuously evaluated for drift and compliance with security baselines. ▪ Defined roles and responsibilities for managing Endpoint and device security.	▪ Endpoint and portable device security processes are fully implemented across the organization and monitored through centralized dashboards. ▪ Decisions are based on prior incidents, threat intelligence, and risk assessments. ▪ Automated alerts for security violations and anomalies involving endpoints and portable devices.	▪ AI and real-time tools are used for optimization and predictive analysis. ▪ Continuous improvement is embedded in workflows and governance. ▪ Advanced analytics for Endpoint and portable device security metrics and performance. ▪ Integration of Endpoint and portable device security with overall

Domain – Technology & Operations				
Sub-Domain – Endpoint and Device Security				
Level 1 – Initial	**Level 2 – Ad-hoc**	**Level 3 – Baseline**	**Level 4 – Advanced**	**Level 5 – Innovative**
installation or media use. ▪ Security incidents originating from endpoints and portable devices are not detected or reported.	device security configurations and risks. ▪ Limited monitoring and reporting of security activities involving endpoints and portable devices. ▪ Antivirus or security agents are deployed on most endpoints, but enforcement and updates vary. ▪ Local firewalls and OS protections are enabled inconsistently. ▪ Some restrictions are applied to external devices (e.g., USB blocking), but not centrally enforced. ▪ Endpoint-related risks are tracked informally or across multiple disconnected tools.	▪ Endpoints and portable devices are largely equipped with security tools such as antivirus, anti-malware and local firewalls. ▪ Implementation of advanced security measures such as endpoint detection and response (EDR) and mobile device management (MDM) across the organization. ▪ Endpoint and portable devices are actively monitored through EDR solutions across the organization users and systems. ▪ Endpoint and portable device configurations are based on a documented hardening baseline (e.g., CIS benchmarks). ▪ Endpoint and portable device logs are collected centrally for high-value or admin machines.	▪ Continuous improvement and refinement of endpoint and portable device security practices based on defined cybersecurity strategy and following the evolvement of threat landscape. ▪ Security events from endpoints and portable devices are correlated with SIEM/XDR and integrated into incident response workflows. ▪ Automated detection and containment actions (e.g., isolation/quarantine) are triggered and conducted on cyber threats from endpoints and portable devices. ▪ Threat hunting is actively performed across endpoint telemetry using advanced analytics.	risk management strategy. ▪ The utilization of AI/ML-based behavioral analysis to detect anomalies and insider threats at the endpoint level. ▪ Device risk scoring is used to dynamically adjust user access and controls in real time. ▪ Endpoint and portable device posture integrates with zero trust access policies and adaptive authentication mechanisms.

Domain – Technology & Operations				
Sub-Domain – Endpoint and Device Security				
Level 1 – Initial	**Level 2 – Ad-hoc**	**Level 3 – Baseline**	**Level 4 – Advanced**	**Level 5 – Innovative**
		▪ USB/media controls and application allowlisting are enforced for sensitive roles. ▪ Asset groups are defined and protected based on business criticality and user function.		

Domain – Technology & Operations				
Sub-Domain – Email Security				
Level 1 – Initial	**Level 2 – Ad-hoc**	**Level 3 – Baseline**	**Level 4 – Advanced**	**Level 5 – Innovative**
▪ Email security processes are ad hoc and undocumented. ▪ Email is delivered without any security filtering or authentication validation. ▪ There are no protections against phishing, spam, spoofing, or malware attachments. ▪ Email gateway logs are not monitored or retained.	▪ Informal Email security practices with minimal documentation. ▪ Basic Email security policies exist but are not consistently enforced. ▪ Limited monitoring and reporting of Email security activities. ▪ Basic email filtering (e.g., spam, malicious links/ attachments, email phishing) is enabled on the email platform. ▪ SPF is configured for selected domains, but	▪ Formalized Email security processes are documented and implemented across all email accounts within the organization. ▪ Regular and continues monitoring and reporting of Email security activities. ▪ Use of Email security tools such as spam filters and anti-malware software. ▪ Inbound and outbound email is filtered through a secure email gateway	▪ Email security processes are fully implemented and monitored using dashboards. ▪ Automated alerts for Email security violations and anomalies are implemented and integrated with the cyber monitoring solutions. ▪ Continuous improvement and refinement of Email security practices.	▪ Continuous improvement is embedded in workflows and governance. ▪ Advanced analytics for Email security metrics and performance. ▪ AI/ML models continuously analyze email metadata, content, and user behavior to identify targeted attacks. ▪ Real-time adaptive warning banners and email risk scoring are

Domain – Technology & Operations				
Sub-Domain – Email Security				
Level 1 – Initial	**Level 2 – Ad-hoc**	**Level 3 – Baseline**	**Level 4 – Advanced**	**Level 5 – Innovative**
	DKIM and DMARC are incomplete or misconfigured. ▪ Attachments and links are scanned inconsistently or only for high-risk users.	(SEG) with anti-malware and anti-spam engines. ▪ SPF, DKIM, and DMARC are fully implemented and aligned with email domain policies. ▪ DMARC policy is enforced (reject/quarantine) and monitored with feedback loops. ▪ Suspicious email reports are triaged by a designated team with documented response procedures. ▪ Basic DLP rules are applied to outbound messages with sensitive content.	▪ Advanced threat protection (ATP) is enabled for zero-day attachments, sandboxing, and link rewriting. ▪ User behavior is monitored for anomalies (e.g., high email volume, unauthorized forwarding). ▪ Email threat intelligence is correlated with SIEM or XDR platforms. ▪ Integrated SOAR workflows automate containment actions (e.g., quarantine, domain block, account isolation). ▪ Incident response playbooks cover business email compromise (BEC), spoofing, and credential phishing.	used per recipient behavior. ▪ Executive and high-risk users are protected by VIP-level controls (e.g., impersonation protection, external message routing review). ▪ Threat intelligence sharing includes email-based IOCs with industry peers and national cyber centers.

Domain – Technology & Operations				
Sub-Domain – Identity and Access Management				
Level 1 – Initial	**Level 2 – Ad-hoc**	**Level 3 – Baseline**	**Level 4 – Advanced**	**Level 5 – Innovative**
▪ No formal access management policy is in place; access is provisioned and revoked in an ad-hoc manner. ▪ Privileged access is inconsistently managed. ▪ User roles and responsibilities are undefined or unclearly documented. ▪ Authentication mechanisms rely on weak passwords without enforcement of minimum length or any other rules. ▪ Segregation of duties is not implemented. ▪ Shared and generic accounts are widely used. ▪ Remote access is not governed by a policy; access is granted without formal structured approval or time limitations. ▪ Logging and monitoring of access activities are either absent or incomplete/inconsistent.	▪ An informal access management policy exists with limited documentation or partial implementation. ▪ Some password policies and role-based access principles are applied, but exceptions are unmanaged. ▪ User access reviews are conducted irregularly. ▪ User lifecycle management is partially implemented and inconsistently followed. ▪ Logging and monitoring of access logs is irregular, and alerts on suspicious activities is reactive. ▪ MFA Is implemented for selected systems only without risk-based or context-aware enforcement.	▪ A documented and approved access management policy is in place, incorporating zero-trust principles, implemented, reviewed annually. ▪ User access provisioning, deprovisioning, and modification are governed by a formal approval and authorization process. ▪ JIT access, context-aware, and risk-based access enforcement are applied consistently. ▪ PAM is implemented to manage privileged users' access. ▪ MFA is applied for all users. ▪ Behavioral analytics tools are used to detect anomalies and trigger security responses. ▪ Access rights are reviewed periodically, based on the user type.	▪ User identity lifecycle and access provisioning are fully orchestrated across on-prem, cloud, and third-party environments through IAM solution. ▪ IAM processes are centralized and automated through an integrated Identity Governance and Administration (IGA) platform. ▪ Access reviews, provisioning, and deprovisioning workflows are fully automated and integrated with HR and IT systems. ▪ Segregation of duties conflicts are proactively identified and remediated through automated access governance tools. ▪ IAM, PAM, and UEBA are fully integrated with SIEM/SOAR for	▪ AI/ML-powered identity analytics are used to continuously assess behavioral patterns to detect anomalies, restrict risky access, and adjust access policies proactively. ▪ AI-powered engines are used to adjust access privileges and session parameters based on contextual risk signals and adaptive trust models.

Domain – Technology & Operations				
Sub-Domain – Identity and Access Management				
Level 1 – Initial	**Level 2 – Ad-hoc**	**Level 3 – Baseline**	**Level 4 – Advanced**	**Level 5 – Innovative**
		▪ Remote access is risk-based and granted via defined policies with enforced MFA and secure channels (e.g., VPN, mTLS), and aligned with zero-trust principles. ▪ Secure password management policies are adopted. ▪ Logging and monitoring of all users' activities are in place and reviewed regularly, with automated alerts configured for suspicious activities.	unified monitoring and automated response.	

Domain – Technology & Operations				
Sub-Domain – Cryptography				
Level 1 – Initial	**Level 2 – Ad-hoc**	**Level 3 – Baseline**	**Level 4 – Advanced**	**Level 5 – Innovative**
▪ Cryptography procedures are ad hoc and undocumented. ▪ No formal Cryptographic policies or frameworks in place. ▪ Encryption is implemented	▪ Informal Cryptographic practices with minimal documentation. ▪ Some effort to follow best practices, but execution is inconsistent.	▪ Formalized Cryptographic policies and procedures with documentation, including approved algorithms and key management practices.	▪ Cryptographic processes are fully implemented and monitored using dashboards. ▪ Comprehensive Cryptographic strategy	▪ Cryptographic processes are proactive, Automated, and data-driven. ▪ AI/ML capabilities are implemented to monitor crypto usage anomalies such as key

Domain – Technology & Operations				
Sub-Domain – Cryptography				
Level 1 – Initial	**Level 2 – Ad-hoc**	**Level 3 – Baseline**	**Level 4 – Advanced**	**Level 5 – Innovative**
inconsistently or not at all across data in transit and at rest. ▪ Legacy or weak cryptographic algorithms may still be in use. ▪ No inventory of cryptographic mechanisms, certificates, or keys exists.	▪ Basic Cryptographic policies exist but are not consistently enforced. ▪ Occasional reviews of Cryptographic configurations and risks. ▪ Basic cryptographic controls are deployed on critical systems. ▪ Some keys are rotated manually, but there is no centralized lifecycle management. ▪ Certificate issuance is decentralized and prone to expiration issues. ▪ No validation of crypto implementation against best practices.	▪ Defined roles and responsibilities for managing Cryptographic practices. ▪ Use of Cryptographic tools such as encryption, hashing, and Digital signatures are defined and implemented across all systems and business units. ▪ Centralized certificate management and key lifecycle tracking (issuance, rotation, revocation) are implemented. ▪ All sensitive data in transit and at rest is encrypted using approved algorithms. ▪ Regular reviews are conducted to identify weak cryptography usage.	and framework with Regular updates. ▪ Quantum-safe cryptography strategy is defined, including pilot adoption of post-quantum algorithms. ▪ Automated alerts are implemented and integrated with the monitoring solutions for Cryptographic violations and anomalies. ▪ Continuous improvement and refinement of Cryptographic practices. ▪ Certificates and keys are auto-renewed, monitored, and tracked via dashboards. ▪ End-to-end encryption is implemented across critical communication and data channels.	misuse and protocol downgrade attempts ▪ Advanced analytics for Cryptographic metrics and performance. Integration of Cryptographic practices with overall risk management strategy. ▪ Cryptographic infrastructure is continuously assessed using automated discovery and compliance tools. ▪ Implementation of Advanced Cryptographic measures such as public key infrastructure (PKI) and quantum-resistant algorithms. ▪ Cryptography posture is visualized across business processes, enabling risk-based key prioritization. ▪ Participate in shaping national or sector-wide

Domain – Technology & Operations				
Sub-Domain – Cryptography				
Level 1 – Initial	**Level 2 – Ad-hoc**	**Level 3 – Baseline**	**Level 4 – Advanced**	**Level 5 – Innovative**
				crypto standards and resilience programs.

Domain – Technology & Operations				
Sub-Domain – Application Security and Secure SDLC				
Level 1 – Initial	**Level 2 – Ad-hoc**	**Level 3 – Baseline**	**Level 4 – Advanced**	**Level 5 – Innovative**
▪ Application security and secure SDLC processes are ad hoc and undocumented. ▪ Minimal understanding of secure coding practices and Application security risks. ▪ Applications are developed or deployed without cybersecurity oversight. ▪ No secure coding standards or formal security checkpoints exist in the development lifecycle. ▪ Security testing is not performed before go-live.	▪ Informal Application security and secure SDLC practices with minimal documentation. ▪ Basic security policies for Application development exist but are not consistently enforced. ▪ Occasional reviews of Application security configurations and risks. ▪ Security reviews are conducted on high-risk applications, often manually or post-development. ▪ Some applications undergo vulnerability scans before release, but findings are inconsistently remediated.	▪ Formalized Application security and secure SDLC framework and processes with documentation. ▪ Regular monitoring and reporting of Application security activities. ▪ Defined roles and responsibilities for managing Application security. ▪ Secure coding guidelines are adopted, and developers receive periodic secure development training. ▪ Applications are subject to static (SAST) and dynamic (DAST) security testing before production release.	▪ Application security and secure SDLC processes are fully implemented and monitored using dashboards. ▪ Automated alerts for application security violations and anomalies. ▪ Continuous improvement and refinement of application security practices. ▪ Implementation of advanced security measures such as dynamic application security testing (DAST) and interactive application security testing (IAST). ▪ Secure SDLC is integrated into CI/CD	▪ Application security and secure SDLC processes are proactive, Automated, and data-driven ▪ AI and real-time tools are used for optimization and predictive analysis. ▪ Continuous improvement is embedded in workflows and governance. ▪ Advanced analytics for Application security metrics and performance. ▪ Use of Advanced technologies like AI/ML code analysis tools to detect contextual vulnerabilities and

Domain – Technology & Operations				
Sub-Domain – Application Security and Secure SDLC				
Level 1 – Initial	**Level 2 – Ad-hoc**	**Level 3 – Baseline**	**Level 4 – Advanced**	**Level 5 – Innovative**
	▪ Third-party libraries or dependencies are used without vetting or patch tracking. ▪ Application documentation lacks clear ownership or security sign-off.	▪ Application architecture is reviewed for security during the design phase. ▪ Threat modeling is performed for new or high-impact applications. ▪ Generate and maintain SBOMs throughout the software lifecycle, ensuring they remain current with all component changes and updates. ▪ Identified vulnerabilities are tracked, prioritized, and resolved through a formal remediation process and through SBOM. ▪ Code repositories and build environments are secured and monitored. ▪ Red team and bug bounty exercises are conducted to assess application defenses.	pipelines with automated SAST/DAST tools and policy gates. ▪ Software composition analysis (SCA) is performed to manage open-source dependencies and license risks. ▪ Application risk scoring is performed and tied to business impact and exposure levels.	guide real-time developer remediation ▪ Secure SDLC maturity is measured continuously across teams and embedded in KPIs. ▪ Application behavior is monitored post-deployment using RASP and telemetry-driven threat detection. ▪ DevSecOps feedback loops enhance security policies dynamically based on emerging attack trends and the threat landscape within the sector.

Domain – Technology & Operations				
Sub-Domain – Change and Release Management				
Level 1 – Initial	**Level 2 – Ad-hoc**	**Level 3 – Baseline**	**Level 4 – Advanced**	**Level 5 – Innovative**
▪ Change and release management processes are ad hoc and undocumented. ▪ No formal schedule or process for Changes and releases. ▪ Changes to systems are made directly in production without formal approval or documentation. ▪ No centralized log or record of system or configuration changes exists. ▪ Releases may introduce downtime, vulnerabilities, or instability without testing. ▪ Cybersecurity is not involved in change decisions or impact assessments. ▪ Emergency changes are handled informally and inconsistently.	▪ Informal Change and release management practices with minimal documentation. ▪ Basic Change and release procedures exist but are not consistently followed. ▪ Changes and releases are performed irregularly and without thorough testing ▪ Some changes are documented post-implementation, but without peer review or cybersecurity input. ▪ Rollback procedures are defined for some systems but are not consistently validated. ▪ There is no change impact analysis related to cyber risk or threat exposure. ▪ Change timing is loosely coordinated with operations or business functions.	▪ A formalized change and release management policy is implemented across all environments. ▪ Changes and releases are tested and reviewed systematically. ▪ Use of Change management tools for tracking and reporting. ▪ All changes are reviewed, approved, and scheduled through a formal Change Advisory Board (CAB) or equivalent process. ▪ Security impact assessments are conducted for infrastructure and application changes. ▪ Rollback plans and test results are required before deployment to production. ▪ A change log is maintained, with traceability to system owners, business impact, and	▪ Change and release management processes are fully implemented and monitored using dashboards. ▪ Comprehensive Change and release management framework with Regular updates. ▪ Automated testing and deployment tools validate configurations and detect policy violations pre-release. ▪ Continuous improvement and refinement of Change and release management practices. ▪ Changes are classified by risk level and require cybersecurity approval for medium/high-risk categories. ▪ Releases follow standardized workflows integrated with CI/CD pipelines, including	▪ Advanced analytics for change success rates and impacts on operations. Change management is adaptive and powered by AI to recommend optimal timing, impact scoring, and automated approval paths. ▪ Real-time visibility into pending, active, and past changes is available via dashboards linked to asset and risk systems. ▪ Self-healing infrastructure rolls back or adjusts failed changes based on telemetry. ▪ Threat intelligence is used to preemptively flag risky changes (e.g., changes to exposed services during global zero-day events).

Domain – Technology & Operations				
Sub-Domain – Change and Release Management				
Level 1 – Initial	**Level 2 – Ad-hoc**	**Level 3 – Baseline**	**Level 4 – Advanced**	**Level 5 – Innovative**
		implementation outcomes.	security testing gates (e.g., SAST/DAST). ▪ Change windows are coordinated across business units with minimal impact to operations. ▪ Post-change reviews evaluate control effectiveness, incidents, and lessons learned.	

Domain – Technology & Operations				
Sub-Domain – Capacity Management				
Level 1 – Initial	**Level 2 – Ad-hoc**	**Level 3 – Baseline**	**Level 4 – Advanced**	**Level 5 – Innovative**
▪ Capacity management processes are ad hoc and undocumented. ▪ Infrastructure and security tools may experience performance degradation or outages during peak load. ▪ Capacity issues are discovered reactively (e.g., during system failure or incident response). ▪ Cybersecurity systems (e.g., SIEM, backup,	▪ Informal Capacity management practices with minimal documentation. ▪ Basic Capacity management policies exist but are not consistently enforced. ▪ Occasional reviews of Capacity configurations and risks. ▪ Limited monitoring and reporting of system and platform's capacity management activities.	▪ Formalized system capacity management processes and plan exists and includes threshold-based monitoring of infrastructure and security systems. ▪ Use of Capacity management tools for tracking and reporting. ▪ A formal capacity management plan exists and includes threshold-based	▪ Capacity management processes are fully implemented and monitored using dashboards. ▪ Automated alerts for Capacity thresholds and anomalies. ▪ Auto-scaling infrastructure supports real-time response to traffic surges or attack loads. ▪ Continuous improvement and	▪ Capacity management processes are proactive, Automated, and data-driven. ▪ AI and real-time tools are used for optimization and predictive analysis. ▪ Advanced analytics for Capacity utilization, forecasting metrics and dynamic resource allocation. ▪ AI/ML models forecast usage patterns and

Domain – Technology & Operations				
Sub-Domain – Capacity Management				
Level 1 – Initial	**Level 2 – Ad-hoc**	**Level 3 – Baseline**	**Level 4 – Advanced**	**Level 5 – Innovative**
endpoint) run with default settings and no scalability plan.	▪ Individual teams perform periodic checks on resource usage (e.g., CPU, memory, storage) for critical systems. ▪ Capacity adjustments are based on user complaints or ad hoc requests. ▪ Security tool performance (e.g., log ingestion, backup retention) degrades silently without alerts.	monitoring of infrastructure and security systems. ▪ Forecasting is performed for key environments (e.g., SIEM storage, backup size, OT control systems). ▪ Reports on utilization trends are reviewed by IT operations and cybersecurity teams. ▪ System upgrades and scaling are planned during defined maintenance windows. ▪ Business-critical systems have documented capacity baselines and buffer policies. ▪ Cybersecurity tools (e.g., endpoint protection, logging platforms) are stress-tested during major change deployments.	refinement of Capacity management practices. ▪ Integration with other IT management systems for holistic oversight. ▪ Capacity monitoring is integrated into centralized dashboards across IT and cloud platforms. ▪ Predictive analytics identify resource exhaustion risks and trigger proactive alerts. ▪ Capacity planning is aligned with DR/BC plans to ensure system resilience during crises. ▪ License utilization and system performance data are factored into procurement and budgeting.	dynamically optimize capacity across hybrid environments. ▪ Capacity telemetry is integrated into threat modeling, DR simulations, and red team scenarios. ▪ Strategic capacity planning includes geopolitical risk, regulatory scaling needs, and technology innovation forecasts. ▪ Collaboration with service providers and peers to benchmark infrastructure and security capacity practices.

Domain – Technology & Operations				
Sub-Domain – Data Protection and Privacy				
Level 1 – Initial	**Level 2 – Ad-hoc**	**Level 3 – Baseline**	**Level 4 – Advanced**	**Level 5 – Innovative**
▪ Data protection and privacy processes are ad hoc and undocumented. ▪ No formal data protection or privacy practices are implemented. ▪ Sensitive data is stored, processed, and shared without classification or access control. ▪ Data retention and destruction are unmanaged and undocumented. ▪ Privacy regulations are either unknown or ignored in daily operations. ▪ No breach response process exists for data exposure or privacy violations.	▪ Informal data protection and privacy practices with minimal documentation. ▪ Basic data protection and privacy policies exist but are not consistently enforced. ▪ Occasional reviews of data protection configurations and privacy risks ▪ Limited monitoring and reporting of data protection and privacy activities. ▪ Some departments apply basic protections (e.g., encryption, access restriction), but without enterprise alignment. ▪ Data protection is addressed reactively — e.g., during audits or after incidents. ▪ Awareness of privacy obligations exists, but policies are fragmented or outdated.	▪ Formalized data protection and privacy policies and processes in place, aligned with regulatory and legal requirements. ▪ Use of data protection tools across the organization such as encryption, access controls, and data loss prevention (DLP). ▪ Data classification schemes are defined and enforced for structured and unstructured data. ▪ Personal data access is role-based, logged, and periodically reviewed. ▪ Data retention and disposal policies are enforced and monitored. ▪ Privacy impact assessments are conducted for high-risk processing or new products.	▪ Data protection and privacy processes are fully implemented and monitored using dashboards. ▪ Automated alerts for data protection violations and privacy breaches. ▪ Continuous improvement and refinement of data protection and privacy practices. ▪ Implementation of advanced measures such as anonymization, pseudonymization, and privacy impact assessments (PIA). ▪ Data discovery and protection tools (e.g., DLP, data masking, encryption) are integrated across all endpoints, servers, and cloud. ▪ Privacy-by-design and privacy-by-default principles are embedded	▪ Real-time data protection is enforced through AI-driven policy engines and behavior-based anomaly detection. ▪ Data governance metrics are tracked live, including access anomalies, retention violations, and consent status. ▪ Synthetic data and PETs (privacy-enhancing technologies) are used in development and analytics. ▪ Customers are provided with transparency dashboards to view and manage their own data rights.

Domain – Technology & Operations				
Sub-Domain – Data Protection and Privacy				
Level 1 – Initial	**Level 2 – Ad-hoc**	**Level 3 – Baseline**	**Level 4 – Advanced**	**Level 5 – Innovative**
	▪ Access to personal or sensitive data is granted manually and not periodically reviewed.	▪ Data breach response procedures include regulatory notification workflows and root cause analysis. ▪ Personal data flows are documented and mapped for regulatory review or internal auditing.	into digital banking and analytics platforms. ▪ Cross-border data transfers are governed by contracts, controls, and approval workflows.	

Domain – Technology & Operations				
Sub-Domain – Logging, Monitoring, and Security Incident Management				
Level 1 – Initial	**Level 2 – Ad-hoc**	**Level 3 – Baseline**	**Level 4 – Advanced**	**Level 5 – Innovative**
▪ Detection and response processes are ad hoc and undocumented. ▪ Security incidents are detected and responded to reactively with minimal oversight. ▪ No centralized logging or security monitoring exists. ▪ Detection is reactive and based on end-user reports or incident aftermath. ▪ There are no defined procedures for triaging,	▪ Informal detection and response practices with minimal documentation. ▪ Basic detection and response policies exist but are not consistently enforced. ▪ Some logs are collected (e.g., firewall, endpoint), but coverage is partial and siloed. ▪ Alerts are generated but reviewed inconsistently or only during audits or compliance checks.	▪ Formalized detection and response frameworks and processes are established. ▪ Defined roles and responsibilities for managing detection and response. ▪ Use of detection tools such as intrusion detection systems (IDS) and security information and event management (SIEM).	▪ Detection and response processes are fully implemented and monitored using dashboards. ▪ Decisions are based on prior incidents, threat intelligence, and risk assessments. ▪ Comprehensive detection and response framework with regular updates. ▪ Automated alerts for security incidents and anomalies.	▪ AI/ML-based analytics detect subtle or unknown threats using behavioral baselines and anomaly scoring. ▪ Detection and response systems adapt dynamically based on business impact, threat actor profiles, or geopolitical risk. ▪ Threat hunting is continuous, proactive, and supported by

Domain – Technology & Operations				
Sub-Domain – Logging, Monitoring, and Security Incident Management				
Level 1 – Initial	**Level 2 – Ad-hoc**	**Level 3 – Baseline**	**Level 4 – Advanced**	**Level 5 – Innovative**
investigating, or responding to alerts. ▪ Security incidents may go undetected for extended periods. ▪ Forensic data is not retained or collected consistently.	▪ Response actions are manual and vary depending on who is available. ▪ Historical logs may be unavailable for investigations or correlation.	▪ A centralized SIEM is deployed to collect logs from key IT and security systems. ▪ Use cases for common threats (e.g., failed logins, malware detection) are defined and maintained. ▪ Alerts are triaged using a documented workflow with defined severity levels and escalation paths. ▪ Detection and response metrics (e.g., mean time to detect/respond) are tracked and reported. ▪ Incident response playbooks are documented and cover key threat scenarios. ▪ Implementation of advanced detection and response measures such as endpoint detection and response (EDR) and network traffic analysis (NTA).	▪ Continuous improvement and refinement of detection and response practices. ▪ Detection use cases are enriched with threat intelligence, behavioral analytics, and contextual data. ▪ Response is partially automated via SOAR (Security Orchestration, Automation and Response) or EDR integrations. ▪ Advanced correlation rules detect lateral movement, privilege abuse, and APT-like behavior. ▪ Post-incident reviews are formally conducted and feed back into detection logic and playbooks.	automated hypothesis testing. ▪ Detection capabilities integrate with network sensors, cloud platforms, and identity providers in a unified XDR framework. ▪ Lessons learned are shared with national CERTs or industry peers to improve sector resilience.

Domain – Technology & Operations				
Sub-Domain – Cybersecurity Testing and Threat Management				
Level 1 – Initial	**Level 2 – Ad-hoc**	**Level 3 – Baseline**	**Level 4 – Advanced**	**Level 5 – Innovative**
▪ Cybersecurity testing and Threat management processes are ad hoc and undocumented. ▪ No structured cybersecurity testing or threat analysis is performed. ▪ Cybersecurity testing and threat management such as vulnerability management, red teaming is limited to informal or compliance-driven scans with no remediation tracking. ▪ Vulnerabilities are discovered reactively — often by external parties.	▪ Informal Cybersecurity vulnerability and patch management practices with minimal documentation of policies and processes. ▪ Basic policies for Cybersecurity testing and Threat management exist but are not consistently enforced. ▪ Basic vulnerability assessments are conducted occasionally on key assets. ▪ Testing is triggered by compliance, new deployments, or external requirements. ▪ Findings are documented but not risk-ranked or tracked to closure.	▪ Formalized Cybersecurity testing and Threat management processes with documentation. ▪ Regular monitoring and reporting of testing outcomes and Threat management activities. ▪ Defined roles and responsibilities for managing testing and Threat management. ▪ Formal cybersecurity testing program exists, including periodic vulnerability scanning and annual penetration testing. ▪ Threat modeling is performed on critical systems during design or major changes. ▪ Testing results are risk-ranked, tracked, and linked to remediation actions. ▪ Cybersecurity testing covers all systems within the IT environment.	▪ Red teaming, purple teaming, or simulated attacks (e.g., phishing, lateral movement) are used to assess detection and response readiness. ▪ Breach and Attack Simulation (BAS) tools are deployed to continuously validate defensive control effectiveness. ▪ Threat exposure is prioritized based on asset criticality, threat actor TTPs (e.g., MITRE ATT&CK), and business impact. ▪ Threat modeling feeds into secure design and change decisions across environments. ▪ Cybersecurity test results inform tuning of SIEM, EDR, and incident playbooks.	▪ A continuous threat exposure management (CTEM) program is in place, aligning testing, detection, and risk mitigation. ▪ AI/ML models simulate attack paths and recommend mitigations in real time. ▪ Testing is fully automated, risk-informed, and tied to cyber risk quantification (CRQ) models. ▪ Threat intelligence, threat modeling, and testing outcomes are unified in a live threat landscape dashboard. ▪ Organization contributes to national threat modeling initiatives, sector-specific attack simulations, or advanced adversary emulation projects.

Domain – Technology & Operations				
Sub-Domain – Cybersecurity Testing and Threat Management				
Level 1 – Initial	**Level 2 – Ad-hoc**	**Level 3 – Baseline**	**Level 4 – Advanced**	**Level 5 – Innovative**
		▪ Threat intelligence is reviewed periodically and linked to risk registers or control reviews.		

Domain – Technology and Operations				
Sub-Domain – Physical and Environmental Security				
Level 1 – Initial	**Level 2 – Ad-hoc**	**Level 3 – Baseline**	**Level 4 – Advanced**	**Level 5 – Innovative**
▪ Physical and environmental security processes are ad hoc and undocumented. ▪ IT server rooms and data centers have minimal or no physical access controls. ▪ Shared keys, open racks, or unmonitored rooms expose critical IT systems to unauthorized access. ▪ Environmental safeguards (e.g., cooling, fire detection) are unmanaged or not tested. ▪ Physical incidents (e.g., theft, overheating) are	▪ Informal Physical and environmental security practices with minimal documentation. ▪ Occasional reviews of Physical security configurations and environmental risks. ▪ Branches and HQ sites implement basic physical controls (e.g., badge access, lock-and-key), but enforcement is inconsistent. ▪ Limited monitoring and reporting of Physical and environmental security activities. ▪ Some surveillance or door access logs are	▪ Formalized Physical and environmental security policies and processes are documented. ▪ Regular monitoring and reporting of Physical security incidents and environmental risks. ▪ Defined roles and responsibilities for managing Physical and environmental security. ▪ Use of Physical security measures such as access controls, surveillance systems, and environmental monitoring tools across the organization. ▪ Access to IT server rooms and data centers	▪ Physical and environmental security processes are fully implemented and monitored using dashboards. ▪ Automated alerts for Physical security breaches and environmental anomalies. ▪ Continuous improvement and refinement of Physical and environmental security practices. ▪ Implementation of Advanced measures such as biometric access controls, integrated security systems, and	▪ Use of advanced technologies to detect anomalies in physical access patterns (e.g., off-hours, access clustering, badge misuse). ▪ Physical security data is correlated in real time with cybersecurity events for holistic threat response. ▪ Badge access is dynamically linked to system access status (e.g., physical access revoked if user offboarded).

Domain – Technology and Operations				
Sub-Domain – Physical and Environmental Security				
Level 1 – Initial	**Level 2 – Ad-hoc**	**Level 3 – Baseline**	**Level 4 – Advanced**	**Level 5 – Innovative**
undocumented and handled ad hoc. ▪ No alignment exists between physical access and IT security policies.	captured but rarely reviewed. ▪ Temperature and power issues are monitored manually or reactively. ▪ Visitors and vendors are logged inconsistently across sites. ▪ Physical controls vary across locations, with no central visibility.	is controlled through electronic systems (e.g., badge readers) with unique IDs and audit logs. ▪ Environmental controls (e.g., UPS, fire suppression, HVAC) are tested and maintained per schedule. ▪ Visitor and vendor access is logged, approved, and periodically reviewed. ▪ Physical access logs are retained and reviewed during security assessments. ▪ Policies align physical access control with IT access provisioning (e.g., joiner/leaver processes).	real-time environmental monitoring. ▪ Central monitoring of physical security controls is in place across data centers and branches. ▪ Surveillance, access control, and environmental systems are integrated with security dashboards. ▪ Access rights are role-based, periodically recertified, and linked to logical access for correlation. ▪ Incident response playbooks include physical breach scenarios (e.g., unauthorized access, tampering). ▪ Environmental alerts (e.g., overheating, power failure) trigger automated notification and logging.	

Domain – Technology & Operations				
Sub-Domain – Cyber Threat Intelligence				
Level 1 – Initial	**Level 2 – Ad-hoc**	**Level 3 – Baseline**	**Level 4 – Advanced**	**Level 5 – Innovative**
▪ Cyber threat intelligence feeds and advisory reports are ingested irregularly without a defined process to action the intelligence information within the cyber protect and defense capabilities. ▪ Cyber threat intelligence feeds and advisory reports are not actively linked to cyber threat monitoring processes and technologies such as SIEM solution, Endpoint and Network Security solutions.	▪ Cyber threat intelligence feeds and advisory reports are ingested on ad-hoc basis and may not be specific to the financial or banking and financial sector or the region within the entity operates. ▪ An informal procedure for actioning the cyber threat intelligence feeds within the cyber threat monitoring processes. ▪ Cyber intelligence feeds and advisory reports are actioned on an ad-hoc basis within the risk assessment and monitoring processes.	▪ Cyber threat intelligence process has been formally defined at Strategic, Tactical and Operational dimensions for identification, analysis, prioritization, and management of cyber threats relevant to the sector and the region. ▪ Cyber threat intelligence process has been formally defined to integrate the ingested cyber intelligence feeds and advisory reports with other cybersecurity processes such as Risk Management, Cyber Monitoring, Cyber Incident Response and others. ▪ Cyber Threat Intelligence platform has been implemented and integrated with cybersecurity solutions to enrich proactive	▪ Cyber Threat Intelligence Strategy and Objectives are defined and aligned with the business and risk priorities. ▪ Cyber threat intelligence capability is implemented with diverse intelligence sources such as industry-specific feeds, deep and dark web and forums monitoring, governmental intelligence with clear mechanism to evaluate reliability and relevance. ▪ Automated processes have been implemented to integrated cyber intelligence platform with other cybersecurity solutions to share feeds in real-time and utilized across all cyber risk assessments, cyber monitoring activities and cyber incident responses.	▪ AI-Driven Cyber Threat Intelligence Lifecycle is implemented through cognitive analytics (GenAI) and large language models to analyze, predict threat evolution, attack paths and hypothesis simulation. ▪ Real-time aggregation and contextualization of structured and unstructured data is implemented from multiple intelligence sources. ▪ Cyber intelligence workflows to update and enrich cyber intelligence processes are implemented through learning from incidents, assessments and simulations. ▪ Proactively share cyber intelligence with the sector peers. ▪ Join Cyber Threat Intelligence sharing

Domain – Technology & Operations				
Sub-Domain – Cyber Threat Intelligence				
Level 1 – Initial	**Level 2 – Ad-hoc**	**Level 3 – Baseline**	**Level 4 – Advanced**	**Level 5 – Innovative**
		threat detection capabilities. ▪ Cyber threat intelligence sharing process has been formally defined to share and receive cyber intelligence with external parties such as CBK and national cybersecurity entities.	▪ Cyber threat modeling and use case development are conducted on regular basis based on threat actor profiling, use case mapping and cyber simulations. ▪ CTI performance metrics and reports are conducted on regular basis to identify areas of enhancement and optimization.	communities (such as ISACS).

Domain – Technology & Operations				
Sub-Domain – Digital Risk Protection				
Level 1 – Initial	**Level 2 – Ad-hoc**	**Level 3 – Baseline**	**Level 4 – Advanced**	**Level 5 – Innovative**
▪ Digital risk protection processes are ad hoc and undocumented. ▪ Minimal understanding of Digital risk protection risks and best practices. ▪ No visibility into cyber threats originating outside the organization's internal perimeter.	▪ Informal Digital risk protection practices with minimal documentation. ▪ Basic Digital risk protection policies exist but are not consistently enforced. ▪ Limited monitoring and reporting of Digital risk protection activities.	▪ Formalized Digital risk protection framework and processes are established. ▪ Regular monitoring and reporting of Digital risk protection activities. ▪ Use of Digital risk protection tools such as Threat intelligence platforms and risk assessment tools.	▪ Digital risk protection processes are fully implemented and monitored using dashboards. ▪ Automated alerts for Digital risk incidents and anomalies. ▪ Implementation of Advanced measures such as Digital footprint monitoring, brand	▪ Digital risk protection processes are proactive, Automated, and data-driven. ▪ Advanced analytics for Digital risk incidents and protection metrics. ▪ AI-enhanced digital risk protection solutions proactively identify emerging threats and

Domain – Technology & Operations				
Sub-Domain – Digital Risk Protection				
Level 1 – Initial	**Level 2 – Ad-hoc**	**Level 3 – Baseline**	**Level 4 – Advanced**	**Level 5 – Innovative**
▪ The organization is unaware of fake domains, phishing attempts, or exposed credentials. ▪ Monitoring of social media, public cloud assets, or third-party exposure is absent. ▪ No process exists to detect or respond to brand abuse or impersonation attempts.	▪ Brand-related incidents are identified reactively (e.g., reported phishing sites, fake social profiles). ▪ Manual checks or informal reports occasionally highlight digital risks. ▪ No formal DRP solution or threat intelligence source is in use. ▪ Digital risk findings are not tracked or responded to systematically.	▪ Brand monitoring / Digital Risk solution or service is implemented to monitor domains, dark web leaks, and impersonation threats. ▪ Phishing domains, brand misuse, and data leaks are detected and reported with takedown requests initiated. ▪ Credential leak monitoring is enabled, and exposed credentials are invalidated. ▪ Alerts from external digital sources are shared with internal teams (e.g., SOC, fraud). ▪ Brand monitoring / Digital Risk monitoring activity is linked to incident response processes and reporting.	protection, and cyber Threat intelligence integration. ▪ Digital risk protection tools are integrated with SIEM, threat intelligence platforms, and fraud detection systems. ▪ Real-time alerts are generated for impersonation, carding activity, or exposed banking infrastructure. ▪ Executive and high-risk personas are monitored for impersonation or targeting. ▪ Takedowns, abuse reports, and platform escalations are tracked with defined SLAs.	cyber campaign patterns. ▪ Continuous mapping of the external attack surface includes rogue apps and misconfigured DNS. ▪ Digital risk protection insights inform risk quantification and business continuity planning. ▪ Organization participates in sector-level collaboration by sharing cyber threat intelligence and insights for faster response to sector-wide cyber threats.

Domain – Third-Party Risk Management and Supply Chain Management				
Sub-Domain – Third-Party Risk Management (TPRM)				
Level 1 – Initial	**Level 2 – Ad-hoc**	**Level 3 – Baseline**	**Level 4 – Advanced**	**Level 5 – Innovative**
▪ No formal TPRM policy exists. ▪ Vendor/third-party selection is based on ad-hoc decisions, without documented due diligence. ▪ Security requirements are not systematically included in contracts. ▪ No accurate or up-to-date inventory or visibility of third-party engagements.	▪ A draft or informal TPRM policy is in place, but inconsistently applied across the Entity. ▪ Risk assessments for third-party vendors are conducted on a case-by-case basis, usually triggered by audits or incidents. ▪ Security requirements or clauses are included in some contracts, but without standardization or any enforcement. ▪ No structured process exists to monitor or re-assess third-party risks regularly.	▪ A formal TPRM policy is in place, approved, and implemented, with the involvement of information security, risk management, and audit functions. ▪ Mandatory due diligence is performed prior to onboarding any third-party IT vendors, covering financial, operational, and cyber and information security aspects. ▪ Contracts and agreements include defined security requirements and clauses, right to audit, and termination provisions. ▪ A complete, accurate, and up-to-date inventory of all third-party agreements is in place. ▪ Periodic assessments (at least annually) are conducted for significant	▪ A centralized TPRM capability/module is implemented (e.g. a GRC platform), enabling standardized processes for due diligence, onboarding, risk assessments, monitoring, and issue tracking across the whole lifecycle. It enables integration of different functions through automated workflows. ▪ Continuous monitoring tools are used to assess vendors' external cyber risk posture (e.g., threat exposure, data breaches, domain spoofing), with dashboards providing real-time risk visibility. ▪ Contracts include dynamic security clauses that are updated in response to changes in the threat landscape or regulatory requirements.	▪ AI/ML is used for early detection of risk indicators across the third-party ecosystem (e.g., financial instability, geopolitical exposure, unusual behavior). ▪ Smart contracts or blockchain-based technologies are used to enforce cyber and information security obligations and monitor compliance in real time.

Domain – Third-Party Risk Management and Supply Chain Management				
Sub-Domain – Third-Party Risk Management (TPRM)				
Level 1 – Initial	**Level 2 – Ad-hoc**	**Level 3 – Baseline**	**Level 4 – Advanced**	**Level 5 – Innovative**
		third-party/outsourcing arrangements. ▪ Continuous monitoring processes are in place to review compliance with security, business continuity, disaster recovery, and data protection clauses. ▪ Gaps in existing agreements are identified and addressed though formal documented remediation measures.		

Domain – Third-Party Risk Management and Supply Chain Management				
Sub-Domain – Supply Chain Risk Management				
Level 1 – Initial	**Level 2 – Ad-hoc**	**Level 3 – Baseline**	**Level 4 – Advanced**	**Level 5 – Innovative**
▪ No visibility into supplier ecosystem or dependencies. ▪ Supply chain risks are not identified or considered as part of the enterprise risk management process.	▪ Supply chain risks are discussed informally during procurement or operational reviews. ▪ Some knowledge of key suppliers exists, but dependency mapping is either incomplete or does not exist.	▪ Suppliers and their dependencies are identified and assessed for risk, with integration into the broader enterprise risk management framework.	▪ Supply chain mapping tools and integrated platforms are used to identify and visualize interdependencies, bottlenecks, and single points of failures across all tiers.	▪ AI/ML-based simulation tools are used to model supply chain disruptions across global networks and test response strategies under varying threat scenarios (e.g., geopolitical

Domain – Third-Party Risk Management and Supply Chain Management				
Sub-Domain – Supply Chain Risk Management				
Level 1 – Initial	**Level 2 – Ad-hoc**	**Level 3 – Baseline**	**Level 4 – Advanced**	**Level 5 – Innovative**
▪ No segmentation or classification of suppliers based on risk or criticality.	▪ Risk mitigation efforts are reactive, usually triggered by incidents or disruptions.	▪ Reliance on single-source suppliers is actively evaluated and minimized via alternative sourcing or backup arrangements. ▪ Suppliers are segmented or classified based on risk and criticality, and enhanced controls are applied to high-risk suppliers. ▪ Real-time monitoring tools and threat intelligence are used to detect issues across the supply chain. ▪ Suppliers are required to flow down security requirements to sub-contractors and fourth parties to maintain consistency.	▪ Supply chain risks are managed through a centralized (e.g. GRC platform) platform, offering visibility into multi-tier supplier dependencies and associated risks. ▪ Sourcing decisions are informed by risk scores, KPIs, and threat intelligence, enabling proactive supplier diversification strategies. ▪ BCP and DRP are extended to include upstream and downstream suppliers, tested through multi-tier simulations.	exposures/tensions, cyber events). ▪ AI-powered supply chain risk intelligence platforms are integrated to build and maintain a dynamic supply chain resilience index, continuously ingesting real-time internal and external risk signals to quantify resilience at the Entity level. ▪ Autonomous decision engines are in place that use predictive analytics and real-time risk inputs to adapt and optimize vendor selection, risk response strategies, and sourcing adjustments without manual intervention.

Domain – Emerging Technologies				
Sub-Domain – Advanced Technologies Security				
Level 1 – Initial	**Level 2 – Ad-hoc**	**Level 3 – Baseline**	**Level 4 – Advanced**	**Level 5 – Innovative**
▪ There is no defined policy or formally	▪ Some informal practices for implementing	▪ A formal policy has been defined for	▪ A strategy has been defined for utilizing	▪ Processes for managing Advanced technologies

Domain – Emerging Technologies				
Sub-Domain – Advanced Technologies Security				
Level 1 – Initial	**Level 2 – Ad-hoc**	**Level 3 – Baseline**	**Level 4 – Advanced**	**Level 5 – Innovative**
documented procedure for implementing emerging technologies. ▪ Minimal understanding of risks and best practices associated with the implementation of emerging technologies.	emerging technologies, but they are not documented or inconsistently applied. ▪ Basic policies for Advanced technology management exist but are not consistently enforced. ▪ Occasional reviews of Advanced technology configurations and risks. ▪ Limited monitoring and reporting of activities involving Advanced technologies.	adopting and implementing new emerging technologies. ▪ Integration between the adoption of emerging technologies with the risk management frameworks is defined and implemented. ▪ Risk assessments, secure code practices and security checks are conducted when developing or implementing systems leveraging the capabilities of emerging technologies. ▪ Cybersecurity controls are defined and implemented to secure emerging technologies from internal and external cyber threats.	emerging technologies such as AI, Blockchain and others to define objectives, integrations, cyber principles and aligned with the business strategy. ▪ Comprehensive framework for the adoption of emerging technologies have been defined and reviewed on regular basis. ▪ Automated alerts for violations and anomalies involving Advanced technologies. ▪ Continuous improvement and refinement of practices for managing Advanced technologies. ▪ Implementation of Advanced measures such as AI-driven analytics, blockchain for secure transactions, and IoT for real-time monitoring.	are proactive, Automated, and data-driven. ▪ AI and real-time tools are used for optimization and predictive analysis. ▪ Continuous improvement is embedded in workflows and governance. ▪ Advanced analytics for metrics and performance of Advanced technologies. ▪ Integration of Advanced technology management with overall risk management strategy. ▪ Use of cutting-edge technologies like machine learning for real-time Threat detection and response, quantum computing for enhanced security, and Automated frameworks for Continuous

Domain – Emerging Technologies				
Sub-Domain – Advanced Technologies Security				
Level 1 – Initial	**Level 2 – Ad-hoc**	**Level 3 – Baseline**	**Level 4 – Advanced**	**Level 5 – Innovative**
				validation and improvement.

Domain – Emerging Technologies				
Sub-Domain – Cloud Security				
Level 1 – Initial	**Level 2 – Ad-hoc**	**Level 3 – Baseline**	**Level 4 – Advanced**	**Level 5 – Innovative**
▪ Cloud security processes are ad hoc and undocumented. ▪ Cloud environments are managed reactively and utilized without a formal policy or defined processes and framework. ▪ Limited or No performance data on Cloud security incidents. ▪ Minimal understanding of Cloud security risks and best practices.	▪ Informal Cloud security practices with minimal documentation. ▪ Some efforts to follow best practices, but execution is inconsistent. ▪ Basic Cloud security policies exist but are not consistently enforced. ▪ Occasional reviews of Cloud security configurations and risks. ▪ Limited monitoring and reporting of Cloud security activities.	▪ Formalized Cloud security processes with documentation. ▪ Regular monitoring and reporting of Cloud security activities. ▪ Risk assessments are conducted to assess the usage of cloud services and establish mitigation measures. ▪ Established Cloud security policies and frameworks. ▪ Defined roles and responsibilities for managing Cloud security. ▪ Threat-informed adjustments begin, but full integration is lacking. ▪ Role-based access controls (RBAC), MFA,	▪ Cloud security processes are fully implemented and monitored using dashboards. ▪ Decisions are based on prior incidents, Threat intelligence, and risk assessments. ▪ Comprehensive Cloud security framework with Regular updates. ▪ Automated alerts for Cloud security violations and anomalies. ▪ Continuous improvement and refinement of Cloud security practices.	▪ Cloud security processes are proactive, Automated, and data-driven. ▪ AI and real-time tools are used for optimization and predictive analysis. ▪ Continuous improvement is embedded in workflows and governance. ▪ Advanced analytics for Cloud security metrics and performance. ▪ Integration of Cloud security with overall risk management strategy.

Domain – Emerging Technologies				
Sub-Domain – Cloud Security				
Level 1 – Initial	**Level 2 – Ad-hoc**	**Level 3 – Baseline**	**Level 4 – Advanced**	**Level 5 – Innovative**
		and encryption-at-rest are enforced for critical cloud services. ▪ Logs from cloud environments are collected in a centralized SIEM. ▪ Third-party risk and shared responsibility are considered in cloud vendor contracts.		

Domain – Payment Security				
Sub-Domain – Common Security Controls for Electronic Payment Systems				
Level 1 – Initial	**Level 2 – Ad-hoc**	**Level 3 – Baseline**	**Level 4 – Advanced**	**Level 5 – Innovative**
▪ No formal policy exists for securing electronic payment systems. ▪ Digital onboarding, authentication, and transaction safeguards are implemented inconsistently or not at all. ▪ Security controls are reactive and fragmented. ▪ Manual identity checks and weak credential	▪ A policy for securing electronic payment systems exists, but is generic, outdated, or lacks implementation guidance and oversight. ▪ Some basic controls for customer onboarding and authentication are in place (e.g., basic ID verification, static passwords). ▪ Limited use of anti-fraud or risk-based mechanisms.	▪ A policy for securing electronic payment systems is formally defined, approved, implemented, reviewed at least annually, and is aligned with industry standards and best practices and regulatory requirements. ▪ Annual and ad-hoc security audits are conducted as per the Cyber Resilience Baselines- Cybersecurity	▪ Automated customer identity verification and onboarding systems utilize API integration with national digital identity platforms (e.g., Kuwait Mobile ID) for real-time validation. ▪ Digital onboarding processes use automated document fraud detection algorithms, such as AI-based OCR anomaly	▪ Implementation of a zero-touch onboarding mechanism leveraging biometric and behavioral profiling, dynamically adapting verification depth based on real-time risk scoring. ▪ Identity proofing and deduplication integrate with national biometric registries or blockchain-based identity solutions, ensuring single identity registration across all

Domain – Payment Security				
Sub-Domain – Common Security Controls for Electronic Payment Systems				
Level 1 – Initial	**Level 2 – Ad-hoc**	**Level 3 – Baseline**	**Level 4 – Advanced**	**Level 5 – Innovative**
handling practices are dominating. ▪ Customer notifications and fraud prevention mechanisms are basic or absent.	▪ Audits are conducted irregularly and are not aligned with standards or best practices. ▪ Encryption and transaction integrity-related controls are applied on selective basis. ▪ Notifications and controls for changes to customer data or payment profiles are implemented inconsistently.	Testing and Threat Management sub-domain, and in line with the requirements of industry standards (e.g., PCI DSS, EMV) and best practices. ▪ Robust digital onboarding mechanisms are in place, including biometric verification, liveness detection, document validation, and cross-checks with authoritative sources. ▪ Multi-Factor Authentication (MFA) is enforced for onboarding and sensitive changes (e.g., mobile number, payee registration). ▪ Device and location-based risk assessments are applied during onboarding and authentication. ▪ Credentials and sensitive information are securely delivered,	detection and tamper detection. ▪ Real-time device posture validation is integrated into onboarding, using device trust scoring prior to permitting system registration. ▪ Credential issuance and delivery processes are managed using automated provisioning tools, enforcing device-specific binding and encryption while at rest and in transit.	financial platforms and channels. ▪ Use of predictive identity risk engines to detect synthetic or high-risk users during onboarding based on behavioral biometrics (e.g., typing patterns), device telemetry, and historical fraud signals. ▪ Seamless authentication orchestration platform is used and is integrated with customer service and different payment channels to enforce adaptive MFA. ▪ End-to-end digital trust framework is implemented using decentralized identity technologies (e.g., Decentralized Identifiers (DIDs)), supporting portable and verifiable credentials.

Domain – Payment Security				
Sub-Domain – Common Security Controls for Electronic Payment Systems				
Level 1 – Initial	**Level 2 – Ad-hoc**	**Level 3 – Baseline**	**Level 4 – Advanced**	**Level 5 – Innovative**
		stored, and encrypted while in transit and at rest. ▪ Failed login limits, secure reactivation procedures, and customer notifications are implemented. ▪ Unique transaction IDs, encryption, and reconciliation mechanism are implemented to ensure payment traceability and integrity. ▪ Customers are provided with self-service options to block cards and receive notifications of significant changes to their payment profiles.		

Domain – Payment Security				
Sub-Domain – Electronic Payment Transaction Monitoring				
Level 1 – Initial	**Level 2 – Ad-hoc**	**Level 3 – Baseline**	**Level 4 – Advanced**	**Level 5 – Innovative**
▪ No formal transaction monitoring process is defined. ▪ Monitoring is manual or limited to basic rule-	▪ A basic monitoring process exists but is not fully aligned with regulatory requirements.	▪ A formal and approved transaction monitoring process is formally defined, implemented, and reviewed at least	▪ Fraud risk management platform is deployed with real-time behavioral analytics and	▪ Real-time and AI-powered customer trust scoring is used to allow, deny, block, or step-up authentication across all

Domain – Payment Security				
Sub-Domain – Electronic Payment Transaction Monitoring				
Level 1 – Initial	**Level 2 – Ad-hoc**	**Level 3 – Baseline**	**Level 4 – Advanced**	**Level 5 – Innovative**
based alerts with no behavioral analysis. ▪ There is no fraud response playbook or documented fraud management process. ▪ Suspicious transactions are not consistently detected, blocked, or escalated. ▪ Customer notifications are not timely or consistently triggered.	▪ Some pre-defined fraud scenarios are detected through static rules. ▪ Response to alerts is inconsistent and largely manual. ▪ Playbooks may exist for some common fraud scenarios but are not reviewed or tested on regular basis. ▪ Alerts and notifications are sent for selected high-value transactions, but coverage is incomplete.	annually, in line with regulatory requirements. ▪ Real-time transaction monitoring is in place, covering the defined risk factors. ▪ Suspicious transactions are automatically blocked or flagged for verification, and they are appropriately logged. ▪ Customers are notified for all transactions, with priority mechanisms for high-risk or abnormal activities using secure offline channels. ▪ A fraud management framework is in place and implemented based on channel, transaction type, and customer risk. ▪ AI/ML-based fraud detection tools are deployed to identify evolving patterns and reduce false positives.	adaptive scoring per customer and device. ▪ Advanced anomaly detection models trained on entity-specific transaction history, leveraging supervised ML models for threshold tuning and contextual decision-making. ▪ Integration of telecom data feeds (e.g., location intelligence, SIM swap indicators) to enhance eSIM-related fraud detection prior to transaction authorization. ▪ All fraud logs and alerts are collected, processed, stored, and correlated in a centralized SOAR platform for automated triaging and incident and case management.	digital/electronic payment channels. ▪ Automated orchestration of response actions via graph-based decision engines, dynamically adjusting fraud mitigation steps based on attack paths and fraud actor techniques. ▪ Integration of voice and video biometric behavior analytics into fraud detection pipeline to detect deepfake fraud or impersonation during onboarding and transaction approvals.

Domain – Payment Security				
Sub-Domain – Electronic Payment Transaction Monitoring				
Level 1 – Initial	**Level 2 – Ad-hoc**	**Level 3 – Baseline**	**Level 4 – Advanced**	**Level 5 – Innovative**
		▪ A fraud response playbook is defined and maintained, that includes a variety of fraud scenarios. ▪ Third-party service providers involved in payment processing are covered in the fraud risk assessment. ▪ The Entity participates in industry-level threat intelligence sharing.		

Domain – Payment Security				
Sub-Domain – Digital Banking Security				
Level 1 – Initial	**Level 2 – Ad-hoc**	**Level 3 – Baseline**	**Level 4 – Advanced**	**Level 5 – Innovative**
▪ Security controls for digital banking services are ad-hoc, inconsistent, or absent. ▪ OTPs, MFA, session management, and device security are either not enforced or loosely implemented. ▪ APIs and Digital Wallet infrastructure lack formal assessment or	▪ Basic authentication (e.g., password, OTP) is implemented for digital banking channels. ▪ Session timeout and device checks are in place, but not uniformly applied or centrally monitored. ▪ Some third-party risk assessments are conducted, and consent	▪ Session timeouts, OTP validity, concurrent session restrictions are implemented for Online and Mobile Banking as per the regulatory requirements. ▪ Strong MFA is enforced for onboarding and critical actions. ▪ Device-level controls (e.g., jailbroken/rooted	▪ Centralized device and session management platform is implemented to monitor and manage all validated devices, enforce revalidation schedules, and enable remote deactivation. ▪ Context-aware adaptive authentication is enabled using device	▪ Graph-based behavioral profiling and decision engines are used to detect abnormal usage patterns, unauthorized API calls, or synthetic user behavior across devices, sessions, and transaction flaws. ▪ Unsupervised AI models that continuously learn and assess user session

Domain – Payment Security				
Sub-Domain – Digital Banking Security				
Level 1 – Initial	**Level 2 – Ad-hoc**	**Level 3 – Baseline**	**Level 4 – Advanced**	**Level 5 – Innovative**
secure development practices. ▪ Required customer consent and awareness around third-party access, OTP preferred delivery method, or digital banking risks are not managed or tracked.	management is partially implemented. ▪ Open Banking API security controls are not fully implemented or monitored. ▪ Limited enforcement of device restrictions or secure transactions validation for Digital Wallets.	detection, device attestation, biometric authentication) are in place across Mobile Banking and Digital Wallets. ▪ Customers can remotely manage and deactivate devices, and all device-related activities are logged and notified. ▪ Periodic security assessments (e.g., Vulnerability Assessments, Penetration Testing) are performed for all digital banking services (e.g., Online/Mobile Banking, Open Banking APIs, and Digital Wallets). ▪ Open Banking APIs are secured through input validation, rate limiting, and real-time monitoring, with detailed logging and consent management, and in line with the	risk scores, time-of-access, behavioral analytics, geolocation, and transaction type. ▪ Secure OTP and biometric authentication are enforced with fallback mechanisms and real-time anomaly detection in delivery patterns (e.g., device mismatch, delayed SMS). ▪ Runtime Application Self-Protection (RASP) is integrated into Mobile Banking Apps to detect and prevent runtime threats in real-time. ▪ Digital Wallet security includes dynamic risk-based transaction controls tied to user behavior and transaction history. ▪ Customer consent management portal is deployed to allow customers modify and	risk in real-time are deployed, flagging or terminating anomalous behavior without relying on pre-trained indicators, to allow for adaptive risk response during user sessions without pre-set rules. ▪ Customers consents and TPP permissions are tracked and managed through tamper-proof mechanisms (e.g., blockchain). ▪ Online and Mobile Banking Applications include AI-powered modules that assess user device's security posture, behavioral patterns, and risk context in real time to drive adaptive authentication and transaction decisions, balancing security with seamless service delivery.

Domain – Payment Security				
Sub-Domain – Digital Banking Security				
Level 1 – Initial	**Level 2 – Ad-hoc**	**Level 3 – Baseline**	**Level 4 – Advanced**	**Level 5 – Innovative**
		relevant regulatory requirements. ▪ Customers are educated on Open Banking risks and consent, permissions, and access management. ▪ Tokenization and secure credential storage are enforced in Digital Wallets.	revoke permissions granted to TPPs.	▪ Autonomous API protection mechanisms are implemented using advanced ML-based threat detection models to

Domain – Payment Security				
Sub-Domain – Payment Card Data Security				
Level 1 – Initial	**Level 2 – Ad-hoc**	**Level 3 – Baseline**	**Level 4 – Advanced**	**Level 5 – Innovative**
▪ There is no formal policy or documented defined procedures for protecting payment card data. ▪ There is no compliance with PCI DSS or other card data security standards (e.g., PCI PTS, PCI SSF, EMV). ▪ Cardholder data (including PAN, PIN, CVV, Cardholder name, expiration date) are stored, processed, or	▪ Some informal practices for protecting card data are in place or partially implemented, but they are not documented or inconsistently applied. ▪ Cardholder data is encrypted or tokenized, but coverage is incomplete or lacks alignment with strong cryptographic standard. ▪ There is no formally documented or enforced policy in place	▪ A formal, documented, and approved payment data protection policy is in place and in line with applicable regulations and industry standards. ▪ A comprehensive inventory of cardholder dataflows is maintained and updated regularly to ensure end-to-end control enforcement. ▪ Cardholder data is encrypted or tokenized both at rest and in	▪ Automated tools are deployed to discover, map, and maintain up-to-date inventories of card dataflows across all systems (on-prem and Cloud), ensuring secure routing and minimizing unauthorized exposure across systems and environments. ▪ Network access to cardholder data is dynamically controlled based on contextual risk	▪ The utilization of Machine Learning (ML) or behavioral analytics to detect anomalies or unauthorized attempts to access or transmit cardholder data. ▪ Real-time risk scoring and adaptive controls are applied to systems processing card data based on sensitivity, user behavior, and exposure.

Domain – Payment Security				
Sub-Domain – Payment Card Data Security				
Level 1 – Initial	**Level 2 – Ad-hoc**	**Level 3 – Baseline**	**Level 4 – Advanced**	**Level 5 – Innovative**
transmitted in an unsecured manner (e.g., unencrypted/not tokenized or improper access controls). ▪ There are no controls in place to prevent the inclusion of the full PAN in communications. ▪ Card PIN generation is insecure, lacking cryptographic protection and controls over secure distribution, access, and management. ▪ Incidents involving payment card data are not captured or analyzed.	to prohibit PAN from being shared in customers communications. ▪ PIN generation uses encryption or hashing, but key management and access controls are undefined or weak. ▪ Monitoring of card data protection in limited or manual; unauthorized exposure may go undetected. ▪ No formal process or procedure exist to validate conformance to PCI-DSS requirements.	transit, using strong approved cryptographic methods. ▪ PIN generation processes follow strong approved cryptographic mechanisms, with strict controls over generation, distribution, and access. ▪ Roles and responsibilities for card data protection are clearly defined and assigned. ▪ Controls are in place to prevent the unauthorized transmission or exposure of cardholder data across systems, application, and communication channels, reinforcing secure handling practices and compliance with internal policies.	factors (e.g., access time, geolocation, device type, large data movements, etc.), with automated triggers for session revocation, reauthentication, or access denial based on pre-defined rules. ▪ Key Risk Indicators (KRIs) related to card data exposure (e.g., encryption failures, blocked transmission attempts, unauthorized access attempts) are tracked and reported to relevant functions.	▪ SOAR platforms with GenAI or intelligent decision engines are used to automate incident analysis (data breaches specifically) and orchestrate context-aware response actions. ▪ Encryption, tokenization, and masking mechanisms are self-healing/self-validating or auto-remediating, correcting misconfigurations or gaps without manual intervention.

Domain – Payment Security				
Sub-Domain – Payment Card Data Security				
Level 1 – Initial	**Level 2 – Ad-hoc**	**Level 3 – Baseline**	**Level 4 – Advanced**	**Level 5 – Innovative**
		▪ Compliance with payment card data protection policies and controls is monitored regularly, with documented review and remediation processes. ▪ Secure PIN management processes and procedures include segregation o duties, tamper-resistant hardware, and cryptographic lifecycle controls. ▪ Employees dealing with and handling card data receive role-based training at least annually.		

Domain – Payment Security				
Sub-Domain – Security of Customer Self-Service Machines				
Level 1 – Initial	**Level 2 – Ad-hoc**	**Level 3 – Baseline**	**Level 4 – Advanced**	**Level 5 – Innovative**
▪ Security measures for customer self-service machines are not documented or inconsistently implemented. ▪ Physical inspections are not or rarely conducted or undocumented. ▪ Card authentication and PIN usage are not standardized, where controls are weak or fragmented. ▪ No controls exist for segregating duties for card processing, PIN generation, card/PIN delivery. ▪ No controls in place for failed PIN attempts.	▪ Basic physical and logical security controls are implemented on some customer self-service machines. ▪ Anti-skimming and tamper detection features may exist, but are not deployed or monitored in a uniform or consistent way. ▪ Physical inspections are conducted irregularly, with limited documentation or remediation tracking. ▪ Segregation of duties for card processing, PIN generation, and card/PIN delivery exist, but lacks oversight or enforcement. ▪ Card block procedures after failed PIN attempts are applied inconsistently across channels.	▪ Physical and logical security controls are consistently implemented on all customer self-service machines. ▪ Physical inspections are conducted at least quarterly and documented, with identified gaps tracked and remediated. ▪ All transactions are authenticated using a combination of card and PIN as applicable. ▪ Segregation of duties is applied and enforced for card processing, PIN generation, and delivery, with card issued in an inactive state and activated securely. ▪ Card is automatically blocked after three failed PIN attempts, and customer is notified immediately.	▪ The Entity centrally manages the entire fleet of customer self-service machines through an integrated platform that enables real-time monitoring, automated fault reporting, automated patching, remote configuration, and centralized policy enforcement across all devices/machines. ▪ Operational and security events from customer self-service machines are integrated with cybersecurity and fraud monitoring systems, to enable real-time detection and cross-channel correlation of anomalies and suspicious activities across physical and digital channels, triggering coordinated incident/fraud response. ▪ Biometric-based fallback authentication is	▪ Advanced technologies such as AI and ML are used to detect anomalies in card usage, PIN entry patterns, and tampering attempts across the self-service machines network. ▪ Predictive analytics are used to schedule proactive inspections and maintenance of customer self-service machines based on location risk profiles, threat intelligence, and usage trends. ▪ Customer self-service machines support proximity-based authentication through mobile devices, using technologies such as NFC or Bluetooth/BLE.

Domain – Payment Security				
Sub-Domain – Security of Customer Self-Service Machines				
Level 1 – Initial	**Level 2 – Ad-hoc**	**Level 3 – Baseline**	**Level 4 – Advanced**	**Level 5 – Innovative**
		▪ Activation of blocked cards follows a defined process with enhanced authentication and verification through secure channels.	implemented on customer self-service machines or via mobile-linked channels to securely support PIN recovery or high-risk transactions. ▪ Dynamic fraud response rules are applied at the customer self-service machine level based on behavioral analytics, to automatically determine whether to proceed, flag, block, or escalate a transaction.	

Domain – Payment Security				
Sub-Domain – Security of Customer Self-Service Machines				
Level 1 – Initial	**Level 2 – Ad-hoc**	**Level 3 – Baseline**	**Level 4 – Advanced**	**Level 5 – Innovative**
▪ Security measures for customer self-service machines are not documented or inconsistently implemented. ▪ Physical inspections are not or rarely conducted or undocumented.	▪ Basic physical and logical security controls are implemented on some customer self-service machines. ▪ Anti-skimming and tamper detection features may exist but are not deployed or	▪ Physical and logical security controls are consistently implemented on all customer self-service machines. ▪ Physical inspections are conducted at least quarterly and documented, with	▪ The Entity centrally manages the entire fleet of customer self-service machines through an integrated platform that enables real-time monitoring, automated fault reporting, automated patching, remote configuration,	▪ Advanced technologies such as AI and ML are used to detect anomalies in card usage, PIN entry patterns, and tampering attempts across the self-service machines network.

Domain – Payment Security				
Sub-Domain – Security of Customer Self-Service Machines				
Level 1 – Initial	**Level 2 – Ad-hoc**	**Level 3 – Baseline**	**Level 4 – Advanced**	**Level 5 – Innovative**
▪ Card authentication and PIN usage are not standardized, where controls are weak or fragmented. ▪ No controls exist for segregating duties for card processing, PIN generation, card/PIN delivery. ▪ No controls in place for failed PIN attempts.	monitored in a uniform or consistent way. ▪ Physical inspections are conducted irregularly, with limited documentation or remediation tracking. ▪ Segregation of duties for card processing, PIN generation, and card/PIN delivery exist, but lacks oversight or enforcement. ▪ Card block procedures after failed PIN attempts are applied inconsistently across channels.	identified gaps tracked and remediated. ▪ All transactions are authenticated using a combination of card and PIN as applicable. ▪ Segregation of duties is applied and enforced for card processing, PIN generation, and delivery, with card issued in an inactive state and activated securely. ▪ Card is automatically blocked after three failed PIN attempts, and customer is notified immediately. ▪ Activation of blocked cards follows a defined process with enhanced authentication and verification through secure channels.	and centralized policy enforcement across all devices/machines. ▪ Operational and security events from customer self-service machines are integrated with cybersecurity and fraud monitoring systems, to enable real-time detection and cross-channel correlation of anomalies and suspicious activities across physical and digital channels, triggering coordinated incident/fraud response. ▪ Biometric-based fallback authentication is implemented on customer self-service machines or via mobile-linked channels to securely support PIN recovery or high-risk transactions. ▪ Dynamic fraud response rules are applied at the customer self-service	▪ Predictive analytics are used to schedule proactive inspections and maintenance of customer self-service machines based on location risk profiles, threat intelligence, and usage trends. ▪ Customer self-service machines support proximity-based authentication through mobile devices, using technologies such as NFC or Bluetooth/BLE.

Domain – Payment Security				
Sub-Domain – Security of Customer Self-Service Machines				
Level 1 – Initial	**Level 2 – Ad-hoc**	**Level 3 – Baseline**	**Level 4 – Advanced**	**Level 5 – Innovative**
			machine level based on behavioral analytics, to automatically determine whether to proceed, flag, block, or escalate a transaction.	

Domain – Payment Security				
Sub-Domain – Contactless Payment Technology Security				
Level 1 – Initial	**Level 2 – Ad-hoc**	**Level 3 – Baseline**	**Level 4 – Advanced**	**Level 5 – Innovative**
▪ No specific controls are in place for securing contactless payment technologies. ▪ NFC, QR, or other contactless payment methods are enabled without prior risk assessment. ▪ No transaction limits are enforced. ▪ Customers do not receive real-time notifications for contactless transactions.	▪ Some contactless payment controls are implemented, but inconsistently across products and channels. ▪ A basic risk assessment is conducted, but controls are not formally documented or reviewed. ▪ Transaction limits for contactless payments are defined but are not actively enforced or monitored. ▪ Customer notifications are sent but are delayed or limited to high-value transactions.	▪ A formal risk assessment is conducted to identify and address the security risks related to NFC, QR, or other contactless payment technologies. ▪ Transaction limits for contactless payments are defined and enforced, and transactions exceeding thresholds require additional/step-up authentication. ▪ Real-time notifications are sent to customers for all contactless payment transactions through effective	▪ Dynamic risk-based authentication is applied for contactless transactions based on real-time behavioral analysis, device posture, and contextual parameters (e.g., transaction velocity, unusual location). ▪ Centralized monitoring platform is in place to track contactless transaction trends, unusual/unexpected device usage, failed attempts, and fraud indicators across all channels.	▪ AI-driven engines are used to autonomously adjust authentication or limits requirements in real-time for contactless transactions, based on federated learning from ecosystem-wide fraud signals, emerging threat vectors, and device behavior. ▪ Context-aware fallback mechanisms are orchestrated in a secure and dynamic way, enabling seamless user experience during disrupted or failed contactless transactions

Domain – Payment Security				
Sub-Domain – Contactless Payment Technology Security				
Level 1 – Initial	**Level 2 – Ad-hoc**	**Level 3 – Baseline**	**Level 4 – Advanced**	**Level 5 – Innovative**
		communication channels. ▪ Contactless security measures and controls are reviewed periodically and updated based on evolving threats.	▪ Adaptive limit controls are applied per customer risk profile, with real-time policy tuning based on emerging threats and fraud trends. ▪ Contactless payments-specific fraud scenarios are included in threat modelling and tested on regular basis through red teaming or other scenario-based exercises.	(e.g., device-based re-authentication, token validation), based on real-time trust scoring.

Domain – Operational Resilience				
Sub-Domain – Business Continuity and Disaster Recovery				
Level 1 – Initial	**Level 2 – Ad-hoc**	**Level 3 – Baseline**	**Level 4 – Advanced**	**Level 5 – Innovative**
▪ No formal BC/DR documentation is in place. ▪ Critical services, supporting systems, and interdependencies are not identified or analyzed. ▪ Backups are ad-hoc, manually managed, and not tested for recoverability or integrity.	▪ Basic BC/DR documentation is in place, but it is not comprehensive, incomplete, unapproved, not reviewed periodically, or poorly communicated. ▪ Identification of critical services, systems, and interdependencies is	▪ A formal and approved BC/DR, BIA, TRA, and Recovery processes and plans are in place across all business units. ▪ Critical services, dependencies, and interdependencies are fully identified and documented. ▪ RTOs, RPOs, and MTDs are defined and approved for all critical	▪ An integrated and centralized GRC platform is used to manage BC/DR plans, testing schedules, recovery requirements, track testing outcomes, and documentation of critical services and interdependencies through automated workflows and risk mappings.	▪ AI/ML-based tools are used to predict service disruptions, simulate recovery strategies, and optimize continuity planning by correlating historical event and incident data, threat intelligence feeds, and environmental indicators. ▪ Dashboards exist to provide

Domain – Operational Resilience				
Sub-Domain – Business Continuity and Disaster Recovery				
Level 1 – Initial	**Level 2 – Ad-hoc**	**Level 3 – Baseline**	**Level 4 – Advanced**	**Level 5 – Innovative**
▪ No alternate recovery site is designated or maintained for critical systems and operations. ▪ RTOs, RPOs, and MTDs are not defined or not aligned with business needs. ▪ There is no defined roles, responsibilities, ownership, or communication protocol for continuity or recovery activities.	initiated, but coverage is partial or outdated. ▪ Backups are performed on a scheduled basis, but recovery testing is infrequent or informal. ▪ An alternate recovery site is designated for some functions, but not tested or maintained consistently. ▪ Preliminary RTOs, RPOs, and MTDs are defined for some systems, but lack validation through testing or business alignment.	systems based on BIA outcomes. ▪ Alternate recovery site is identified and geographically separate from the primary site, with defined roles, equipment, and connectivity are established and tested annually ▪ Regular backups are performed, with testing conducted on quarterly basis to validate data integrity and recovery effectiveness. ▪ Annual testing (e.g., failovers, recovery drills, tabletop exercises) is conducted with documented results and corrective actions. ▪ Roles and responsibilities for continuity and recovery are defined and communication.	▪ Communication protocols, stakeholder roles, call trees, and escalation paths are automated through the GRC platform. ▪ Updates to BC/DR plans are triggered automatically based on changes in business processes, IT architecture, or third-party dependencies. ▪ Real-time operational risk indicators (e.g., backup failures, service degradation, upstream disruptions) are integrated into executive dashboards for proactive decision-making. ▪ Advanced simulations model complex multi-layered and sector-specific scenarios (e.g., hybrid cyber and physical attacks, cascading vendor failures/supply chain	Executive/Senior Management with real-time and forward-looking visibility into resilience posture, recovery readiness, testing outcomes, predictive risk indicators, and emerging risks. ▪ Digital twin models or virtual replicas of critical business functions are maintained to simulate response and validate recovery under changing threat conditions. ▪ Resilience insights are continuously refined using ML to improve accuracy of RTOs and RPOs identification across systems and services.

Domain – Operational Resilience				
Sub-Domain – Business Continuity and Disaster Recovery				
Level 1 – Initial	**Level 2 – Ad-hoc**	**Level 3 – Baseline**	**Level 4 – Advanced**	**Level 5 – Innovative**
		▪ Escalation and communication protocols are defined. ▪ Executive/Senior Management reviews tests outcomes, approves plans, and sign off on resolution of gaps.	disruptions, regional outages, cloud disruption). ▪ Specialized dependency mapping tools are used to visualize and manage internal/external service interdependencies, failover chains, and supply chain components. ▪ BC and DR testing results are integrated and linked to the enterprise risk dashboards.	

Domain – Operational Resilience				
Sub-Domain – Cyber Crisis Management				
Level 1 – Initial	**Level 2 – Ad-hoc**	**Level 3 – Baseline**	**Level 4 – Advanced**	**Level 5 – Innovative**
▪ No formal or documented cyber crisis management plan exists; response to crisis is reactive and uncoordinated. ▪ Undefined roles and responsibilities for Crisis Management Team (CMT).	▪ Informal cyber crisis management plans are drafted, but lack approval, organization-wide alignment, or compliance with legal and regulatory requirements. ▪ A CMT is identified, but no clear definition of roles, cross-functional	▪ Cyber crisis management plans are formally documented, approved, implemented, reviewed periodically –or upon a significant change- and updated. ▪ A designated, qualified, and trained CMT exists, with defined roles and	▪ Crisis management planning is integrated into a centralized GRC platform, enabling automation of updates, task assignments, tracking and monitoring, severity mapping, escalation workflows, and stakeholder	▪ AI/ML tools are used to analyze historical data, identify hidden patterns, and proactively predict potential crises before they occur. ▪ ML is leveraged to continuously monitor for emerging trend, anomalies, and behavioral shifts,

Domain – Operational Resilience				
Sub-Domain – Cyber Crisis Management				
Level 1 – Initial	**Level 2 – Ad-hoc**	**Level 3 – Baseline**	**Level 4 – Advanced**	**Level 5 – Innovative**
▪ There is no documented process for classifying incidents severity and escalating to crisis-level. ▪ No training or testing-related to cyber crisis scenarios is conducted. ▪ Communication with stakeholders during crisis is ad-hoc and unstructured.	composition, or decision-making authority. ▪ Incident reporting processes are inconsistent; timelines and escalation procedures are not formalized. ▪ Some cyber crises are documented, but lessons learnt are rarely incorporated into updates. ▪ Limited internal training and testing exercises may occur, but it is unstructured, scope is incomprehensive and lacks involvement from critical business units.	responsibilities for all functions. ▪ A severity impact matrix is in place and approved. ▪ Incident notification and reporting to CBK follows the mandated timelines and communication templates. ▪ Cyber crisis exercises are conducted on regular basis. ▪ Lessons learnt from crises and exercises are documented and inform updates to the crisis management plans and other processes and controls.	communication protocols. ▪ CMT operates based on pre-defined playbooks, supported by automation/digital tools that streamline coordination, decision logging, and status reporting. ▪ Real-time dashboards are in place to provide situational visibility to leadership during crisis. ▪ Scenario-based testing simulates complex hybrid crisis and includes participation of critical third parties.	signaling potential cyber threat or crisis trigger. ▪ Real-time data from multiple sources is collected and processed using AI tools to provide dynamic and enterprise-wide visibility, enabling faster and informed decisions. ▪ AI-powered sentiment analysis is used to assess social media and public communication channels to gauge reputational impact and identify areas of concern during a crisis. ▪ AI-driven decision engines are utilized to enable automated response recommendations, calibrated to the severity and nature of the incident, risk tolerance and appetite, and historical effectiveness. ▪ Crisis simulation platforms powered by

Domain – Operational Resilience				
Sub-Domain – Cyber Crisis Management				
Level 1 – Initial	**Level 2 – Ad-hoc**	**Level 3 – Baseline**	**Level 4 – Advanced**	**Level 5 – Innovative**
				AI/ML are used to model hybrid crisis scenarios and enhance readiness through continuous testing and adaptation. ▪ AI tools are used to optimize allocation of resources during crises. ▪ AI-powered chatbots and virtual assistants are used to support real-time communication, situation updates, and guidance for CMT. ▪ Post-crisis insights are generated automatically, to identify lessons learnt and areas of improvement. ▪ AI/ML capabilities are integrated with the centralized GRC platform, enabling unified, intelligent, and adaptive crisis management.

10.2 Appendix B – Operational Resilience Baselines

This appendix presents the maturity attributes across each domain of the CBK Operational Resilience Baselines

Domain – Governance and Oversight				
Level 1 – Initial	**Level 2 – Ad-hoc**	**Level 3 – Baseline**	**Level 4 – Advanced**	**Level 5 – Innovative**
▪ No formal operational resilience policy, strategy, or governance structure is in place. ▪ The Board, or equivalent, and the Executive/Senior Management are not actively engaged in operational resilience policy oversight. ▪ Roles, responsibilities, and escalation paths for resilience are undefined or fragmented. ▪ The Operational Resilience Function, if present, lacks independence, mandate, and authority. ▪ Compliance obligations are not tracked; no register of applicable legal or regulatory requirements is maintained.	▪ An operational resilience strategy or policy exist, but is generic, outdated, or not approved at the appropriate level. ▪ Board Involvement is irregular and limited to reactive updates or attestation requests. ▪ Roles and responsibilities are partially defined but not fully aligned or monitored. ▪ A Resilience Steering Committee may exist but lacks a charter, quorum, or cross-functional participation. ▪ The Operational Resilience Function exists but is embedded within other departments and lacks accountability across domains.	▪ A formal operational resilience strategy and policy are defined, aligned with regulatory and business requirements, approved, communicated, and reviewed at least annually. ▪ Roles, responsibilities, and accountability documented across Board, Committee, Executives and OR Function. ▪ The Resilience Steering Committee is formally established with a documented charter, meets quarterly, and chaired by a qualified senior executive with the relevant knowledge and skills. ▪ Board or delegated committees approve	▪ An automated tool that is used for managing operational resilience policy full lifecycle, including development, review, approval, publication, and version control, ensuring consistency, traceability, and alignment with legal and regulatory requirements. ▪ Approvals, delegations, and decision-making processes are tracked through automated workflows. ▪ Compliance management is centralized and technology-enabled solution for automated monitoring of regulatory changes (e.g., alerts and notifications), and linked to risk registers	▪ Advanced methods and emerging practices are applied to enhance decision-making and strategic oversight, enabling intelligence-driven, predictive, and continuously optimized operational resilience governance. (e.g., AI auto-maps regulatory controls to organizational frameworks, ensuring instant alignment with new rules and eliminating manual mapping efforts). ▪ Advanced capabilities are applied to provide real-time insights, identify governance anomalies, and recommend corrective actions (e.g., highlighting delayed approvals, policy

Domain – Governance and Oversight				
Level 1 – Initial	**Level 2 – Ad-hoc**	**Level 3 – Baseline**	**Level 4 – Advanced**	**Level 5 – Innovative**
	▪ Regulatory compliance tracking is inconsistent, with ad-hoc awareness of key obligations and minimal updates.	strategy, allocate budgets, and receive regular updates. ▪ The Operational Resilience Function is independent, empowered by the Board, and leads cross-domain resilience execution. ▪ Regular reporting is provided to the Board, or equivalent, on operational resilience status, risks, and emerging threats. ▪ A compliance register is maintained and updated annually, covering regulatory and best practice requirements aligned with ISO 22301 and CBK expectations.	for unified GRC oversight.	misalignments, or gaps in risk tolerance). ▪ The Board and Resilience Steering Committee are supported with interactive and real-time insights that enhance visibility into disruption risk exposure, policy performance, and the effectiveness of governance controls. ▪ Advanced approaches to automate compliance mapping, impact workflows, evidence collection, reporting, and certification tracking processes.

Domain –Risk and Threat Management				
Level 1 – Initial	**Level 2 – Ad-hoc**	**Level 3 – Baseline**	**Level 4 – Advanced**	**Level 5 – Innovative**
▪ No formal risk assessment methodology is in place; activities are reactive and undocumented. ▪ Disruption risks are not systematically identified, tracked, or evaluated for potential disruption. ▪ There is no centralized risk register; threat types (internal, external) are not consistently analyzed. ▪ Treatment plans are absent or informal, and risk monitoring is not conducted. ▪ Roles and responsibilities for risks are not defined across business or technology teams. ▪ There is no assignment of risk or control ownership; no accountability framework exists.	▪ A basic risk assessment methodology exists but is applied inconsistently across the entity. ▪ Risk assessments are performed on an ad-hoc basis, typically driven by audits, incidents, or regulatory triggers. ▪ Disruption risks are identified sporadically, with unclear ownership, severity evaluation, or treatment categories. ▪ A risk register may exist but lacks comprehensive coverage, regular updates, or standardized threat taxonomy. ▪ Treatment responses (accept, avoid, transfer) are discussed case-by-case without formal tracking. ▪ Reporting is irregular, and updates to senior management are reactive. ▪ Threats are recognized/identified reactively; there is no	▪ A formal, documented, and approved risk assessment methodology is implemented and aligned with industry standards and best practices. ▪ The methodology clearly outlines the scope, frequency, roles and responsibilities, and execution of risk assessments. ▪ Risk assessments are conducted at least annually or whenever triggered by defined change or threat scenarios. ▪ Risk identification includes internal/external disruption threats and evaluates impact, likelihood, and control effectiveness. ▪ Risks are documented in a centralized risk register, including those	▪ Risk management is fully integrated across the Entity and aligned with the Entity's overall Enterprise Risk Management (ERM) framework. ▪ Emerging threats are proactively monitored using structured threat intelligence feeds, industry reports, and disruption risk insights. ▪ Control effectiveness is continuously measured and monitored, with periodic testing and performance reviews (at least quarterly). ▪ An automated tool that is in place to manage the entire risk lifecycle, with utilization of capabilities for risk scoring, workflow-based treatment tracking, and automated alerts or escalations based on predefined timeline or severity thresholds.	▪ Risk and threat management are predictive, data-driven, and tightly integrated with enterprise governance (e.g., actively supports strategic and transformation initiatives across the Entity). ▪ Analyze historical incidents, external threat intelligence, and operational data to predict threats and recommend governance adjustment in real-time. ▪ A horizon scanning model is implemented to provide early warnings of emerging risks by analyzing external intelligence, industry signals, and global events, with outputs linked directly to Key Risk Indicators (KRIs) for proactive monitoring.

Domain –Risk and Threat Management				
Level 1 – Initial	**Level 2 – Ad-hoc**	**Level 3 – Baseline**	**Level 4 – Advanced**	**Level 5 – Innovative**
	threat monitoring process.	affecting outsourced sites. ▪ Consolidated risk reporting is provided to the Resilience Steering Committee at least annually. ▪ Risk treatment plans are categorized, documented, justified, tracked and monitored for completion.		▪ Maintain real-time visibility into risk posture, treatment progress, and control performance. ▪ Risk insurance policy is regularly reviewed, strategically managed and optimized, considering evolving threats, exclusions, and financial exposure (ROI analysis and active claims monitoring).

Domain – Business Continuity Management				
Level 1 – Initial	**Level 2 – Ad-hoc**	**Level 3 – Baseline**	**Level 4 – Advanced**	**Level 5 – Innovative**
▪ No formal BIA methodology is applied. ▪ Critical services, supporting processes and single points of failure (SPOFs) are not identified. ▪ Recovery strategies are undefined, and alternate sites are not considered. ▪ Business Continuity Plans (BCPs) are not	▪ A basic BIA methodology exists. ▪ Critical services, supporting processes and SPOFs are inconsistently identified across all departments and not comprehensively reviewed or documented or tracked. ▪ Basic identification of resource requirements	▪ A BIA methodology is defined, implemented, and reviewed annually or upon significant change. ▪ Critical services, supporting processes, SPOFs, and recovery resource requirements are identified and mapped. ▪ Identification of resource requirements	▪ An automated tool that is utilized to manage and streamline BIA and BCP workflows and recovery strategy selection, improving accuracy, traceability, and response times. ▪ Critical systems' business RTOs and RPOs are regularly compared against their corresponding IT RTCs	▪ Maintain real-time visibility into critical services and supporting processes. enabling leaders to quickly identify issues and make proactive decisions. ▪ Perform advanced analysis to identify comparisons and discrepancies between

Domain – Business Continuity Management				
Level 1 – Initial	**Level 2 – Ad-hoc**	**Level 3 – Baseline**	**Level 4 – Advanced**	**Level 5 – Innovative**
developed or maintained. ▪ Resources and internal dependencies are not identified.	and internal dependencies but not comprehensively documented or maintained. ▪ Recovery strategies are considered on a case-by-case basis without structured evaluation. ▪ BCPs exist for select departments but lack regular updates, review, or formal approval processes.	and internal dependencies are mapped between departments. ▪ Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs) are defined for critical systems. ▪ BCPs are developed and maintained for all departments, reviewed annually, and contain the required plan components. ▪ BIA results and SPOFs are consolidated by the Operational Resilience Function and reported to the Resilience Steering Committee. ▪ Recovery strategies are maintained and updated based on MAO/MTPD, RTOs, and RPOs, including alternate geographically separate recovery sites, with selection and approval by the	and RPCs to identify and address discrepancies.	business RTOs and RPOs and IT RTCs and RPCs.

Domain – Business Continuity Management				
Level 1 – Initial	**Level 2 – Ad-hoc**	**Level 3 – Baseline**	**Level 4 – Advanced**	**Level 5 – Innovative**
		Resilience Steering Committee.		

Domain – Technology Resilience				
Level 1 – Initial	**Level 2 – Ad-hoc**	**Level 3 – Baseline**	**Level 4 – Advanced**	**Level 5 – Innovative**
▪ No formal TIA methodology is applied. ▪ No formal backup strategy or disaster recovery plan exists for critical IT systems. ▪ Backup frequency, storage location, and recovery requirements are undefined. ▪ IT systems and infrastructure dependencies are not identified or documented. ▪ High availability, capacity planning, and service-level objectives are not considered. ▪ No structured approach to resilience in service lifecycle or recovery objectives.	▪ A basic TIA methodology exists. ▪ DRP exists but lacks regular updates, review, or formal approval processes. ▪ Backup processes exist for some systems but are inconsistently applied or undocumented. ▪ Backup testing is occasional and not aligned with organizational recovery objectives. ▪ Some awareness of critical systems exists, but dependencies and RTO/RPO are not fully defined. ▪ Resilience considerations are sporadically included in IT architecture or	▪ A TIA methodology is defined, implemented, and reviewed annually or upon significant change. ▪ DRP is developed and maintained, reviewed annually, and contain the required plan components. ▪ A formal backup is defined, implemented and reviewed annually or upon significant changes. ▪ Backup strategy includes defined frequence, secure storage/disposal, and testing of critical systems. ▪ High availability configurations are implemented for critical systems; service-level	▪ An automated tool that is utilized to manage and streamline TIA, DRP workflows and IT recovery selections, improving accuracy, traceability, and response times. ▪ Systems are proactively monitored for usage, depreciation, and incidents through automated tools that provide real-time visibility and alerts to support timely recovery actions. ▪ Application interdependencies are continuously analyzed, with recovery objectives (RTOs) compared across applications to ensure alignment and minimize impacts.	▪ Continuously monitor system performance, depreciation, and usage while integrating incident data to provide real-time insights. ▪ Consolidate real-time data on applications, infrastructure, and dependencies to provide leadership with a holistic view of resilience posture. ▪ Advanced analytics compare RTOs with dependent applications, identifying misalignments and recommending corrective adjustments before disruptions occur.

Domain – Technology Resilience				
Level 1 – Initial	**Level 2 – Ad-hoc**	**Level 3 – Baseline**	**Level 4 – Advanced**	**Level 5 – Innovative**
▪ Disaster Recovery Plan (DRP) are not developed or maintained.	service support decisions. ▪ Some reactive consideration of resilience, with limited monitoring and irregular reviews.	objectives are defined and monitored. ▪ Resilience requirements embedded in core service processes, with defined recovery objectives and periodic reviews. ▪ Technology requirements meet RTO and RPO that are identified in the BIA. ▪ Backup and restoration processes are aligned with business priorities and tested annually for selected systems. ▪ The TIA and DRP are consolidated and reported by the Operational Resilience Function to the Steering Committee. ▪ A geographically separate DR site is established with infrastructure aligned to recovery timeframes. ▪ Availability and integrity of IT systems are monitored		

Domain – Technology Resilience				
Level 1 – Initial	**Level 2 – Ad-hoc**	**Level 3 – Baseline**	**Level 4 – Advanced**	**Level 5 – Innovative**
		continuously; service reviews are conducted regularly and used for improvement.		

Domain – Incident and Crisis Management				
Level 1 – Initial	**Level 2 – Ad-hoc**	**Level 3 – Baseline**	**Level 4 – Advanced**	**Level 5 – Innovative**
▪ There is no formal incident or crisis management structure or defined response teams. ▪ Plans for managing disruptive events are not documented or consistently followed. ▪ Internal communication during incidents is informal and lacks predefined channels or responsibilities. ▪ There is no escalation or reporting structure to CBK based on severity tiers. ▪ No impact classification criteria or response protocols are defined or adopted.	▪ Initial incident response structures exist but are inconsistently activated or defined across teams. ▪ Crisis and incident plans may be drafted but are not reviewed, approved. ▪ Communication protocols are manually coordinated, with limited predefine responsibilities or tools. ▪ CBK reporting is reactive and may not follow formal timing, escalation, or closure requirements. ▪ The severity impact matrix, although provided, has not yet been fully adopted or	▪ A three-layered response structure is established (Crisis Management, Incident Management, and Incident Response Teams) with activation criteria tied to impact severity. ▪ Incident and crisis management plans are approved by the Steering Committee, aligned with regulatory and operational requirements, and reviewed annually. ▪ Internal and external communication responsibilities are assigned, with mass communication tools in place.	▪ A unified incident management framework ensures that all types of incidents, which may currently follow separate processes, are centralized under a single, streamlined approach, enhancing consistency, visibility and response efficiency. ▪ Enable automatic incident reporting and integrate a centralized ticketing system, ensuring all incidents are captured, tracked, and resolved within a single platform. This improves visibility, reduces duplication, and supports faster	▪ Capture and organize incident details with minimal manual input, reducing reliance on manual documentation. ▪ Utilize a tool to instantly distributes tailored messages to stakeholders through multiple communication channels (e.g., SMS, email, apps). ▪ Utilize advanced technologies to analyze scenarios and recommend response actions based on impact, risk, and past events. ▪ Consolidate and visualize real-time incident data, impact

Domain – Incident and Crisis Management				
Level 1 – Initial	**Level 2 – Ad-hoc**	**Level 3 – Baseline**	**Level 4 – Advanced**	**Level 5 – Innovative**
▪ No severity impact matrix defined. ▪ There is no Crisis Command Center.	embedded into day-to-day decision-making. ▪ Crisis Command Center chosen but not equipped with the necessary tools to respond to a crisis.	▪ CBK reporting follows defined timelines for initial notification, updates and closure based on severity. ▪ The provided severity impact matrix has been adopted and embedded into decision-making. ▪ Communication teams and spokespeople are pre-assigned, with protocols tested during simulations. ▪ Crisis Command Center is established with the necessary tools to respond to a crisis.	response and accountability. ▪ Playbooks are developed directly from risk assessment results, ensuring that the CMT and Strategic Leadership Team have tailored, scenario-based guidance aligned with identified vulnerabilities. ▪ Crisis Command Center is established and integrated with CBK, enabling 24/7 real-time monitoring, communication and connectivity for coordinate crisis response.	analysis, and response progress to support command and decision-making. ▪ Continuously track the operational health and security of infrastructure, feeding real-time data into the risk management framework to enable proactive early warnings.

Domain – Testing, Training, and Continuous Improvement				
Level 1 – Initial	**Level 2 – Ad-hoc**	**Level 3 – Baseline**	**Level 4 – Advanced**	**Level 5 – Innovative**
▪ No formal testing exercises. ▪ No formal training is being conducted for employees.	▪ Some testing activities (e.g., tabletop or awareness sessions) are performed but lack consistency or structured objectives.	▪ Tabletop, BCP/DRP, and partial crisis simulations are conducted annually (only strategic layer) to test decision-making	▪ Fully fledged crisis simulation is conducted annually (tactical and strategic layer) to test decision making and resilience capability.	▪ Wargaming is conducted at the executive and strategic levels to simulate large-scale crises and stress-test leadership decision-

Domain – Testing, Training, and Continuous Improvement				
Level 1 – Initial	**Level 2 – Ad-hoc**	**Level 3 – Baseline**	**Level 4 – Advanced**	**Level 5 – Innovative**
▪ Lessons learned and post-exercise improvements are not being captured. ▪ Training needs are not being analyzed or addressed.	▪ Documentation of exercise results and lessons learned is incomplete and not incorporated. ▪ Awareness training is provided to some employees, but coverage is limited and unsystematic. ▪ Crisis simulation scenarios are generic or reused without alignment to current risks. ▪ There is no formal mechanism to report results to the Steering Committee or update plans based on test outcomes. ▪ Partial training needs analysis is conducted, but coverage is limited.	and resilience capabilities. ▪ Test scenarios are realistic, defined with objectives and cover critical processes, alternate site functionality, and end-to-end recovery. ▪ Awareness and specialized training are conducted at least annually, including for contractors and relevant third parties. ▪ Lessons learned are documented and incorporated. ▪ Training needs analysis is conducted regularly. ▪ Results are reported to the Resilience Steering Committee; evidence of training and assessments is retained. ▪ Sectorial crisis management exercises are implemented.	▪ Specialized crisis simulation platforms are leveraged to design and execute realistic, end-to-end exercises, enabling organizations to validate response strategies, enhance coordination and measure readiness across functions. ▪ Key vendors and partners actively participate in resilience exercises to validate dependencies and coordinated response. ▪ Exercises are designed around the most pressing and emerging risks, ensuring relevance and strategic value.	making under complex, high-pressure scenarios. ▪ Create an immersive and realistic crisis environment that allow employees to practice response actions in a safe setting. (e.g., Senior leaders are placed in VR and AR-based drills, reinforcing procedures and improving retention of critical actions). ▪ Integrate feedback mechanisms into training to evaluate performance and highlight strengths and weaknesses. ▪ Replicate operations and critical systems in simulated environments to test resilience strategies against evolving threats. (e.g., The digital twin simulates the impact of potential disruptions on critical operations,

Domain – Testing, Training, and Continuous Improvement				
Level 1 – Initial	**Level 2 – Ad-hoc**	**Level 3 – Baseline**	**Level 4 – Advanced**	**Level 5 – Innovative**
				enabling proactive testing and refinement of recovery strategies before real incidents occur).

10.3 Appendix C – Third-Party Risk Management Baselines

This appendix presents the maturity attributes across each domain of the CBK Third-Party Risk Management Baselines.

Domain – Governance Structure and Oversight				
Level 1 – Initial	**Level 2 – Ad-hoc**	**Level 3 – Baseline**	**Level 4 – Advanced**	**Level 5 – Innovative**
• No formal TPRM governance structure is defined or implemented. • Roles and responsibilities for TPRM are undefined, unclear, or undocumented. • Board and Executive/Senior Management are not involved in TPRM oversight. • TPRM policy and strategy are absent or exist in a draft form. • No formal committee or designated functions exists for TPRM governance. • Reviews and approvals for TPRM documents (i.e., policy, strategy, risk assessments) are	• TPRM policy and strategy exist but lack alignment with business objectives or regulatory requirements. • Roles and responsibilities are partially defined, but not fully communicated or understood. • Executive/Senior Management provides limited oversight and Board involvement is minimal or informal. • A designated TPRM function or committee may exist but is not formally mandated or empowered. • Reviews and updates to the policy and strategy occur sporadically or in reaction to issues.	• A formal TPRM policy and strategy are I place, approved, and reviewed annually and upon changes in the third-party landscape. • The Board approves the strategy and attests the policy, ensuring alignment with regulatory mandates and risk appetite. • A TPRM oversight committee is established, chaired by a senior executive, with formal charter and cross-functional membership. • Senior management oversees the implementation and operationalization of the framework, allocates adequate resources, and	• TPRM governance and oversight activities are automated through a centralized GRC platform, enabling structured policy and strategy management, automated workflows, and exceptions tracking. • A comprehensive set of KPIs and KRIs are established to monitor policy compliance and gap remediation timeliness. • Real-time dashboards provide consolidated and holistic visibility to the Board, Executive/Senior Management, and oversight functions on risk posture, vendor tiers, compliance status, and strategic roadmap	• TPRM strategy and policy are continuously enhanced through AI-driven insights, using data from internal systems, third-party behavior analytics, and external threat feeds to dynamically adjust objectives, thresholds, and roadmap priorities. • The Board, TPRM Oversight Committee, and Executive/Senior Management are supported by AI-enabled dashboards and decision support tools, surfacing high-impact risks, non-compliance trends, and deviations from strategic objectives. • Predictive threat intelligence and macro-risk signals are synthesized, enabling

Domain – Governance Structure and Oversight				
Level 1 – Initial	**Level 2 – Ad-hoc**	**Level 3 – Baseline**	**Level 4 – Advanced**	**Level 5 – Innovative**
informal or undocumented. • Reviews of TPRM documents are not conducted or they are reactive and conducted only in response to incidents or external triggers.	• Collaboration among departments exist but is informal or not structured.	integrates TPRM with ERM and BCP. • Periodic reporting to the Board and Executive/Senior Management is conducted, covering posture, emerging threats, and remediation. • The TPRM is function is fully established, staffed with multidisciplinary expertise, and responsible for consistent implementation. • All approval, reviews, and updates are documented with traceable audit trails.	implementation progress. • Risk assessments and associated reviews are continuously updated based on threat intelligence and evolving risk profiles. • Review cycles are risk-tiered, and compliance is proactively validated. • TPRM strategy is dynamically informed by internal and external threat intelligence, which is used to re-assess third-party risk ratings, adjust risk acceptance thresholds, and identify emerging systemic risks.	anticipatory discussions and strategy adjustments. • AI/ML models are leveraged to prioritize review cycles based on predictive indicators, regulatory changes, or external events.

Domain –Risk Management Framework				
Level 1 – Initial	**Level 2 – Ad-hoc**	**Level 3 – Baseline**	**Level 4 – Advanced**	**Level 5 – Innovative**
• Third-party risk is not formally identified or assessed. • No classification of third-party services	• Initial third-party inventories exist but are incomplete or outdated. • Risk assessments are performed inconsistently and only	• A centralized and updated inventory of all third-party relationships is maintained, with critical vendors clearly flagged and integrated	• Third-party risk assessments and tiering are automated via a centralized GRC tools, with integrated workflows for periodic	• Third-party risk scoring is enhanced with AI/ML-based predictive models, analyzing trends in vendor failure, threat landscapes,

Domain –Risk Management Framework				
Level 1 – Initial	**Level 2 – Ad-hoc**	**Level 3 – Baseline**	**Level 4 – Advanced**	**Level 5 – Innovative**
based on criticality or data sensitivity. • There is no inventory of third-party services and their relationships or dependencies. • Risk assessments are informal, unstructured, and reactive. • Business Continuity Plans (BCPs) do not consider third-party failures or dependencies.	for selected vendors or are undocumented. • Criticality is determined based on business intuition rather than a defined criteria. • Due diligence is informal, limited to onboarding only, or lacks tiering or consistent updates. • Dependency mapping is incomplete, not systematic, or unlinked to BCPs.	with the BCP and risk register. • Third-party criticality is determined using defined criteria, including impact on critical business services, data sensitivity, and regulatory/operational dependencies. • Risk assessments are conducted using a multi-dimensional methodology, covering financial, legal, cyber, reputational, and regulatory risks. • Risk scoring and tiering are applied using qualitative and quantitative techniques, driving prioritization, of due diligence and monitoring. • Due diligence is performed at onboarding and reviewed periodically based on vendor tier and performance indicators. • Dependency mapping identifies single point of	reviews, escalations, and approvals. • KPIs and KRIs ae defined and monitored to track risk exposure, remediation timelines, control effectiveness, and third-party performance. • Dependency mapping is visualized in real-time, highlighting upstream/downstream vendor linkages, systemic vulnerabilities, and cascading failure scenarios. • The third-party inventory is integrated with enterprise architecture, service maps, and BIAs to ensure alignment with resilience mapping, and automated via a GRC platform. • Real-time threat intelligence feeds are used to trigger re-assessments and re-tiering of third parties dynamically.	geopolitical risks, and performance anomalies. • AI/ML tools are used to predict vendor risks and automatically simulate cascading failure impacts. • Advanced dependency simulations model operational, geographic, and data interlinkages, enabling proactive identifications of critical failure points across the ecosystem. • Critical third parties are involved in joint continuity drills and resilience testing exercises, validating readiness and recovery capabilities.

Domain –Risk Management Framework				
Level 1 – Initial	**Level 2 – Ad-hoc**	**Level 3 – Baseline**	**Level 4 – Advanced**	**Level 5 – Innovative**
		failures and interdependencies, which are embedded in BCPs and DRPs.	• Findings from third-party risk assessments and dependency mapping directly inform scenario-based testing of BCP and disaster recovery strategies. `	

Domain – Contractual Agreements and Considerations				
Level 1 – Initial	**Level 2 – Ad-hoc**	**Level 3 – Baseline**	**Level 4 – Advanced**	**Level 5 – Innovative**
• Contracts with third parties are often informal, missing, or lack consistency in clauses and execution. • No structured legal review or formal signatory process is applied before contract execution. • There is no centralized contract repository; contracts are stored in silos with limited access or version control. • EHS, ABAC, or financial health clauses are generally absent or handled verbally.	• Standard contract templates exist but are applied inconsistently and without full legal review. • Some contracts include basic clauses (e.g., confidentiality, SLAs), but critical ones (e.g., audit rights, sub-contractor controls) are often omitted. • A partially consolidated contract repository exists but is not comprehensive or audit ready. • EHS and financial viability provisions are included for selected vendors only.	• All third-party engagements are governed by legally binding and duly executed contracts, reviewed by legal counsel, including enforceable clauses for core provisions (e.g., scope, audit, termination, liability, dispute resolution, data handling, SLAs, confidentiality, etc.). • A centralized and access-controlled contract repository is maintained and updated, covering all PO, non-PO, and one-	• Contract lifecycle activities are automated through a centralized platform (e.g., Contract Lifecycle Management (CLM) system), supporting clause libraries, deviation alerts, approval workflow, and renewal tracking. • KPIs and KRIs are defined and linked to contractual clauses and terms. • Contractual compliance monitoring is triggered by real-time risk signals, including threat intelligence, vendor	• AI-driven CLM platforms are used to assess clauses completeness and enforceability, identifying missing risk provisions, outdated regulatory references, or weak liability terms. • Predictive analytics are applied to forecast contract failure risks (e.g., SLA collapse, financial insolvency, data breach liability) and trigger renegotiations or mitigation strategies. • Smart contracts and blockchain-enabled audit trails are used in

Domain – Contractual Agreements and Considerations				
Level 1 – Initial	**Level 2 – Ad-hoc**	**Level 3 – Baseline**	**Level 4 – Advanced**	**Level 5 – Innovative**
• No regular monitoring of contractual compliance or performance obligations.	• Oversight of compliance with contractual terms is reactive and undocumented.	time vendor engagements. • Contracts include structured provisions for EHS, financial viability reviews, ABAC compliance, and disclosure of regulatory and litigation risks. • A documented monitoring process is in place to evaluate vendor performance against SLAs, KPIs, legal obligations, and sub-contractor arrangements. • Periodic financial and compliance checks are conducted, based on contractual clauses, paths defined for non-compliance. • Investigations, unresolved violations, or regulatory audits of vendors are documented and incorporated into TPRM oversight activities.	incidents, or regulatory changes. • Third parties are required to maintain and share updated ABAC, EHS, and compliance registers, which are periodically reviewed by the Entity. • Governance, litigation, and regulatory exposures are linked to the contract review cycle, ensuring continuity clauses and exit triggers are kept current. • Contracts include enforceable obligations for back-to-back risk transfer to subcontractors, including cybersecurity specific clauses, with visibility and control mechanisms built in.	high-risk/vendor-critical cases. • The Entity participates in contract intelligence-sharing ecosystems, benchmarking clauses effectiveness and SLA failure trends. • Scenario testing and tabletop exercises validate the enforceability of key contract provisions (e.g., data return, escrow access, liability execution) under crisis conditions. • Contracts adapt automatically to regulatory and geopolitical changes through integrated legal intelligence. • High-risk parties are required to demonstrate live compliance with EHS and ABAC requirements through digital attestations, telemetry,

Domain – Contractual Agreements and Considerations				
Level 1 – Initial	**Level 2 – Ad-hoc**	**Level 3 – Baseline**	**Level 4 – Advanced**	**Level 5 – Innovative**
				or regulator-facing audits.

Domain – Risk Assessment and Monitoring				
Level 1 – Initial	**Level 2 – Ad-hoc**	**Level 3 – Baseline**	**Level 4 – Advanced**	**Level 5 – Innovative**
• Risk assessment and monitoring activities are informal, reactive, and inconsistently applied across the organization. • Formal documentation and standardized processes for risk assessment and monitoring are not established. • Risk-related decisions are made without fully considering potential threats, disruptions, or the broader organizational risk context	• Risk assessment and monitoring practices are ad-hoc, with partial documentation and inconsistent adoption across the organization. • Risk controls and monitoring mechanisms are fragmented, with limited coordination and accountability, leading to gaps in oversight and response. • Performance metrics and monitoring processes are inconsistent or unreliable, hindering effective assessment and continuous improvement of risk management practices.	• Comprehensive documentation of risk assessment standards, monitoring procedures, and policies is established, regularly reviewed, and aligned with legal and regulatory requirements. • Risk assessments, threat intelligence, and business impact analyses are integrated into security planning, with proactive implementation of risk controls and monitoring mechanisms. • Performance metrics and dashboards are used to assess compliance, monitor risk controls, and incorporate insights from past incidents and	• Risk assessment and monitoring processes are streamlined and automated, and aligned with business goals, enhancing operational efficiency and responsiveness. • Real-time monitoring and advanced analytics provide enterprise-wide visibility into emerging risks and performance, enabling proactive risk management. • Continuous improvement is driven by data-driven insights, with processes optimized to leading practices through ongoing refinement and automation.	• Risk assessment and monitoring are anticipatory and intelligence-led, leveraging real-time risk indicators, predictive modeling, and AI to enable proactive management. • Cutting-edge technologies like AI and machine learning are integrated into risk management, providing predictive analysis, automated responses, and strategic decision support. • Risk management is aligned with evolving business needs and sector developments, driven by real-time monitoring.

Domain – Risk Assessment and Monitoring				
Level 1 – Initial	**Level 2 – Ad-hoc**	**Level 3 – Baseline**	**Level 4 – Advanced**	**Level 5 – Innovative**
		emerging trends for continuous improvement.		

Domain – Business Continuity Management and Disaster Recovery				
Level 1 – Initial	**Level 2 – Ad-hoc**	**Level 3 – Baseline**	**Level 4 – Advanced**	**Level 5 – Innovative**
• Business continuity and disaster recovery are informal and reactive, resulting in inconsistent practices that hinder timely recovery. • There is a lack of formal documentation for business continuity and disaster recovery standards, leading to a fragmented approach and uncoordinated responses during critical events. • Decision-making reflects risk awareness but lacks an integrated approach, delaying recovery and impacting operations during incidents.	• Documentation is incomplete and fragmented, with no formal integration, resulting in a reactive approach to disruptions and inconsistent application of disaster recovery controls. • Business continuity and disaster recovery efforts are siloed and misaligned across departments, with unclear accountability and unimplemented plans to meet regulations and best practices. • Post-incident reviews are inconsistent, and performance metrics are unreliable or absent, limiting the ability to assess and	• Comprehensive documentation, risk assessments, and business impact analyses are regularly reviewed and aligned with evolving risks and regulatory requirements to ensure robust disaster recovery planning. • A proactive, structured approach is maintained through the consistent application of baseline recovery controls and integration of insights from incidents, exercises, and emerging trends to improve recovery capabilities. • Legal, regulatory, and industry standards are met, with performance metrics and dashboards	• Business continuity and disaster recovery processes are centralized, automated, and aligned with organizational goals, improving efficiency, control, and ensuring critical operations are prioritized. • Real-time monitoring, advanced analytics, and predictive tools enable early identification of risks, streamline recovery, and ensure proactive, timely responses to emerging disruptions. • Continuous improvement is driven by performance data, maturity assessments, and lessons learned,	• Business continuity and disaster recovery are anticipatory, using real-time risk indicators, advanced threat modeling, and cutting-edge technologies like AI and ML for predictive analytics and adaptive recovery strategies. • Practices are dynamically aligned with evolving risks, organizational priorities, and sector-specific developments to ensure timely, effective recovery • AI-powered monitoring systems provide real-time situational awareness and insights, while the organization actively engages in

Domain – Business Continuity Management and Disaster Recovery				
Level 1 – Initial	**Level 2 – Ad-hoc**	**Level 3 – Baseline**	**Level 4 – Advanced**	**Level 5 – Innovative**
	improve recovery effectiveness.	regularly used to monitor compliance, effectiveness, and support continuous improvement.	optimizing recovery processes for future	sector-wide innovation, collaboration, and resilience initiatives.

Domain – Incident Management				
Level 1 – Initial	**Level 2 – Ad-hoc**	**Level 3 – Baseline**	**Level 4 – Advanced**	**Level 5 – Innovative**
• Incident management is informal, reactive, and inconsistently applied, leading to delayed responses and elevated operational risk. • The absence of formal standards and procedures results in unstructured and ineffective disruption responses. • Risk awareness exists but is not systematically integrated into incident response decision-making.	• Incident management practices are ad-hoc, poorly documented, and lack standardization or institutional adoption across the organization. • Controls are inconsistently applied, with siloed efforts, limited coordination, and unclear accountability hindering effective and cohesive response. • Post-incident reviews, data retention, and performance monitoring are inconsistent or absent, limiting oversight, improvement, and regulatory alignment.	• Incident management is governed by regularly reviewed documentation, aligned with risks, regulations, and organizational priorities. • Risk assessments and threat intelligence drive proactive response planning, prioritizing critical functions and implementation of baseline controls. • Continuous improvement is supported by lessons learned, regulatory compliance, and ongoing performance monitoring through established metrics.	• Incident management is centralized and automated to enhance consistency, efficiency, and timely response across the organization. • Real-time monitoring, advanced analytics, and automated workflows enable early threat detection, enterprise-wide visibility, and improved responsiveness. • Incident response is strategically aligned with business objectives and driven by data-informed continuous improvement, supported by predictive tools and maturity assessments.	• Incident management is proactive, leveraging real-time data, threat modeling, and AI/ML for predictive and autonomous decision-making. • Incident practices align with evolving risks, business priorities, and sector developments, supported by real-time dashboards that provide leadership with actionable insights. • The organization leads sector-wide innovation, intelligence sharing, and collaboration, enhancing collective resilience and continuous improvement.

Domain – Data Protection and Confidentiality				
Level 1 – Initial	**Level 2 – Ad-hoc**	**Level 3 – Baseline**	**Level 4 – Advanced**	**Level 5 – Innovative**
• Risk management activities are informal, reactive, and inconsistently applied across the organization. • There is no formal documentation or standardized processes for managing data protection and confidentiality. • Decisions are made without clear consideration of potential data risks, threats, or broader organizational impact.	• Documentation and practices for data protection are partial, inconsistent, and not standardized across the organization. • 2. Data protection controls are fragmented, with limited coordination across teams, and ad-hoc plans to meet regulatory requirements remain unimplemented. • 3. Incident response and data retention practices are inconsistent, and performance metrics are either unreliable or absent, hindering effective monitoring and improvement.	• Comprehensive documentation for data protection and confidentiality is in place, regularly reviewed, and aligned with legal, regulatory, and industry standards. • Risk assessments, threat intelligence, and business impact analyses inform the proactive implementation of data protection controls and monitoring. • Continuous improvement is driven by incident learnings, performance metrics, and dashboards to evaluate and enhance the effectiveness of data protection measures	• Data protection processes are centralized, automated, and aligned with the organization's business strategy, improving efficiency and operational integration. • Real-time monitoring and advanced analytics provide enterprise-wide visibility into data risks, enabling early detection and proactive responses. • Continuous improvement is driven by automated workflows, performance metrics, and ongoing optimization based on insights from analytics and maturity modeling. • Cross-border flow mapping, just-in-time access controls, and predictive retention	• Data protection practices are anticipatory and intelligence-led, using real-time risk indicators and predictive threat modeling to proactively manage risks. • Advanced technologies like AI and machine learning enable predictive analysis, automated responses, and dynamic adaptation to business needs, regulatory changes, and sector developments. • AI-powered dashboards provide continuous situational awareness, supporting data-driven decision-making and contributing to sector-wide innovation and collaboration in data protection.

Domain – Data Protection and Confidentiality				
Level 1 – Initial	**Level 2 – Ad-hoc**	**Level 3 – Baseline**	**Level 4 – Advanced**	**Level 5 – Innovative**
			scheduling are enabled across third parties.	

Domain – Sub-Contracting				
Level 1 – Initial	**Level 2 – Ad-hoc**	**Level 3 – Baseline**	**Level 4 – Advanced**	**Level 5 – Innovative**
• Third-party sub-contracting arrangements are not documented or disclosed. • There is no formal requirement for sub-contractor approval or risk assessment. • There is no visibility into sub-contractors ("nth parties") or their roles in service delivery.	• Some third parties disclose the use of sub-contractors, but disclosures are incomplete or triggered only upon request. • Approvals for sub-contractors are informal or inconsistent, and typically handled reactively. • Risk assessments of sub-contractors are rarely performed, unless issues arise. • Contract may mention sub-contractors, but there is no consistent requirement for signed sub-contracting agreements or oversight clauses.	• Third parties are required to disclose and obtain prior approval from the Regulated Entity before engaging and sub-contractors, including for new or changed scopes of service. • Signed sub-contracting agreements between third parties and their sub-contractors are mandated and verified during onboarding. • Sub-contractors undergo risk assessments proportional to the criticality of their roles and access to systems, data, or customer impact. • Documented policy and procedures for managing sub-	• All sub-contractors are subject to formal approval workflows, embedded in automated systems that enforce policy-driven validation before onboarding or scope changes. • Continuous monitoring and periodic re-assessments of sub-contractors are conducted. • Sub-contractor data is integrated into centralized TPRM platforms, feeding vendor risk registers, reporting dashboards, and audit reporting.	• AI-powered tools monitor sub-contacting chains in real-time, assessing nth-party risks and flagging concentration and systemic risks. • Predictive models are used to help proactively assess high-risk sub-contracting practices (e.g., overreliance on key providers, geopolitical exposures) and recommend mitigation strategies before the fact.

Domain – Sub-Contracting				
Level 1 – Initial	**Level 2 – Ad-hoc**	**Level 3 – Baseline**	**Level 4 – Advanced**	**Level 5 – Innovative**
		contracting risks, including identification of "nth parties". • Oversight of subcontracted vendors is included as part of the overall third-party monitoring process.		

Domain – Exit Strategy				
Level 1 – Initial	**Level 2 – Ad-hoc**	**Level 3 – Baseline**	**Level 4 – Advanced**	**Level 5 – Innovative**
• No defined process exists for off-boarding, deactivating, or blacklisting third-party vendors. • Termination clauses are inconsistently included or entirely absent in third-party contracts. • No knowledge transfer or data handling process is conducted during third-party exit.	• Off-boarding processes exist but are informal and inconsistently applied across engagements. • Some agreements include termination clauses but lack clarity or enforceability. • Knowledge transfer is done informally with no documentation or accountability.	• Third parties are off boarded using a formalized checklist and standardized process based on defined exit scenarios. • Exit and termination clauses are included in all contracts, ensuring clear disengagement procedures. • Knowledge transfer sessions and data purging/destruction requirements are part of the formal exit checklist, including secure deletion protocols.	• Exit plans are customized based on risk tiering and service criticality and include scheduled knowledge transfer and system deactivation steps. For high-risk vendors, the Regulated Entity initiates an early exit simulation to validate the readiness of backup providers and recovery plans. • Smart contract templates include auto-enforcement of termination terms based on SLA violations or expiration. When a	• Exit planning is predictive and integrated with contract lifecycles, using analytics to auto-trigger pre-exit actions and initiate risk mitigation workflows. The Regulated entity automates secure exits through a TPRM tool that enforces off-boarding workflows, collects data disposal certificates, revokes access rights, and ensures encrypted transfer of retained knowledge base. • Use of contract lifecycle management (CLM)

Domain – Exit Strategy				
Level 1 – Initial	**Level 2 – Ad-hoc**	**Level 3 – Baseline**	**Level 4 – Advanced**	**Level 5 – Innovative**
			vendor breaches availability SLAs, a pre-configured smart clause triggers a notification and initiates disengagement workflows automatically. • Certificates of deletion and structured data handover formats are mandated and audited as part of the exit report. During offboarding, the vendor is required to submit a disposal certificate and conduct a formal walkthrough of all retained system configurations.	tools to dynamically manage third-party exit terms with legal validation and AI-based clause recommendations. The legal and TPRM teams use a CLM platform that suggests optimized termination clauses based on risk profile and past engagements. • Enforced use of automated workflows that include secure deletion, audit trails, and regulatory mapping of data purging obligations.

Domain – Storage of Data				
Level 1 – Initial	**Level 2 – Ad-hoc**	**Level 3 – Baseline**	**Level 4 – Advanced**	**Level 5 – Innovative**
• Data storage practices are informal, reactive, and inconsistently applied across the organization.	• Data storage documentation is partial and inconsistent, with practices not fully standardized or	• Storage controls, encryption at rest, retention policies, and storage hygiene practices are enforced	• Data storage and lifecycle controls are risk-based, embedded across the third-party ecosystem with	• AI/ML is used to detect abnormal storage access and predict data risks across all third-party storage layers.

Domain – Storage of Data				
Level 1 – Initial	**Level 2 – Ad-hoc**	**Level 3 – Baseline**	**Level 4 – Advanced**	**Level 5 – Innovative**
• No formal documentation or standardized processes exist for data storage. Data storage decisions are made without full awareness of disruption risks or organizational context.	institutionalized across the organization. • Data protection controls are fragmented and lack coordination, with informal and unimplemented plans to align with regulatory standards. • Data retention practices are inconsistent, and performance metrics for data storage are unreliable, hindering effective monitoring and improvement.	with clear accountability. • key management, configuration, redundancy, access management, and logging are implemented and subject to periodic reviews and audit trails. • Backup and DR procedures are tested.	proactive enforcement, centralized dashboards, and automation. • Encryption keys have rotation policies. Cloud and on-prem storage use segmentation, tagging, and monitoring. • Storage locations and media are classified and inventoried. • Retention and deletion processes are enforced automatically. • A Regulated Entity requires third parties to integrate cloud-native storage with automated classification and tagging of data sensitivity levels (e.g., public, confidential, restricted), triggering automated encryption, logging, and purge actions. Immutable storage is used for logs, and segmented zones	• Real-time decisions are made to encrypt, segment, or archive data automatically. Immutable logs, DR capabilities, and storage resiliency mechanisms are tightly integrated and self-healing. • Regulated Entity enables its critical third-party core service provider to leverage AI-based anomaly detection for storage access patterns. If a sensitive dataset is accessed unusually, the system automatically revokes access, logs the event immutably, and triggers a secondary DR copy sync in an isolated vault while notifying compliance teams in real time.

Domain – Storage of Data				
Level 1 – Initial	**Level 2 – Ad-hoc**	**Level 3 – Baseline**	**Level 4 – Advanced**	**Level 5 – Innovative**
			protect backup vaults and critical repositories.	

Domain – Cross-Boarder Transaction				
Level 1 – Initial	**Level 2 – Ad-hoc**	**Level 3 – Baseline**	**Level 4 – Advanced**	**Level 5 – Innovative**
• Cross-border transaction controls are ad-hoc, undocumented, and reactive. • Lack of formal procedures for screening, documentation, or regulatory validation. Reliance on manual approvals.	• Basic procedures exist for cross-border payments, but practices vary across departments. • Limited due diligence is performed manually. • No centralized oversight or integration with CBK-sanctioned channels.	• Cross-border transactions are routed through approved payment systems with documented procedures for sanctions screening, LEI validation, due diligence, and compliance reporting. • Periodic audits are conducted, and key records are maintained.	• Advanced Cross-border compliance processes are fully integrated with centralized transaction systems. • Automated screening tools are in place for sanctions, LEI, licensing, and risk-based due diligence. • All activities are logged with tamper-evident records. Regulatory reports and audits are submitted within required timelines. • Regulated Entity integrates real-time screening of all cross-border transactions using an automated solution that checks against UN, US, EU, and FATF lists. The system also flags transactions	• The institution leverages AI/ML for predictive risk scoring of cross-border activities, enabling proactive alerts before transactions are initiated. Audit trails support immutable records. • Fully integrated dashboards monitor payment channels, due diligence, and export/import compliance in real-time. • The Entity deploys AI-driven anomaly detection models to predict high-risk counterparties for tamper-proof audit trails of large transactions. The system also auto-generates compliance

Domain – Cross-Boarder Transaction				
Level 1 – Initial	**Level 2 – Ad-hoc**	**Level 3 – Baseline**	**Level 4 – Advanced**	**Level 5 – Innovative**
			from high-risk jurisdictions and triggers workflow approvals for EDD.	reports and flags suspicious patterns to regulators.

Domain – Usage of Cloud Services				
Level 1 – Initial	**Level 2 – Ad-hoc**	**Level 3 – Baseline**	**Level 4 – Advanced**	**Level 5 – Innovative**
• Cloud service activities are informal, reactive, and inconsistently applied, causing fragmented risk mitigation and delayed response. • No formal documentation exists for cloud-specific standards, policies, or procedures, resulting in governance and compliance gaps. • Cloud adoption and incident decisions consider some risks but lack an integrated, organization-wide approach.	• Cloud security documentation is incomplete, and practices are ad-hoc, non-standardized, and not institutionally adopted. • Cloud controls are inconsistently implemented, with siloed efforts and unclear accountability limiting cohesive risk management. • Post-incident analysis, data retention, and performance monitoring are unreliable or absent, impeding oversight and improvement	• Cloud security standards and procedures are formally documented, approved, and regularly reviewed to address evolving risks and regulations. • Cloud-specific risk assessments and threat intelligence inform proactive response planning, prioritizing critical cloud functions and baseline controls. • Continuous improvement incorporates cloud incident learnings, regulatory compliance, and ongoing performance monitoring via cloud-	• Cloud security processes are centralized and automated, ensuring consistent and efficient cloud operations management. • Real-time monitoring and advanced analytics provide enterprise-wide visibility into cloud risks, performance, and service health. • Automated cloud workflows and alerts enhance incident response efficiency, aligned with business continuity objectives and supported by data-driven continuous improvement.	• Cloud security is anticipatory and intelligence-led, leveraging real-time indicators, advanced threat modeling, and AI/ML technologies for predictive analytics and adaptive response. • Cloud practices dynamically align with evolving risk appetites, business priorities, and sector developments, supported by AI-powered awareness dashboards. • The organization actively participates in sector-wide cloud innovation, information sharing, and collaboration,

Domain – Usage of Cloud Services				
Level 1 – Initial	**Level 2 – Ad-hoc**	**Level 3 – Baseline**	**Level 4 – Advanced**	**Level 5 – Innovative**
		specific metrics and dashboards.		strengthening industry-wide robustness.

Domain – Inter-Affiliates				
Level 1 – Initial	**Level 2 – Ad-hoc**	**Level 3 – Baseline**	**Level 4 – Advanced**	**Level 5 – Innovative**
• No formal approval, due diligence, or monitoring process exists for affiliate engagements. • Customer consent and geopolitical considerations are not addressed.	• Approval from the CBK is obtained on a case-by-case basis. • Basic due diligence is performed for high-risk affiliates. • Minimal documentation exists for customer consent or business continuity with affiliates.	• Standard procedures are established for approval and due diligence of affiliates. • Periodic reviews and SLAs are in place. Customer consent for data sharing is implemented. • Foreign affiliate controls are aligned with internal standards.	• Centralized oversight over all affiliate engagements, with automated due diligence tracking and SLA performance dashboards. • Customer consent is seamlessly integrated with core systems. • Business continuity planning includes affiliate dependencies. • Usage of centralized third-party risk platform that triggers automated due diligence reviews and SLA validations for all affiliates, including monitoring geopolitical risks for its regional operations in high-risk zones.	• AI-driven analytics are used to assess affiliate risk in real-time, including geopolitical tensions, SLA performance trends, and consent violations. • Decision-making on affiliate onboarding and renewal is data-driven aligned with risk appetite. • Integrates a geopolitics risk feed into affiliate monitoring system, which uses machine learning to flag high-risk regions. When a foreign affiliate's risk exceeds threshold, automated workflows notify compliance and restrict data sharing pending review.

Chapter 4:
Cyber Resilience Baselines

DOCUMENT CONTROL

Date	Version	Author	Change Reference	Reviewer/ Approver
03 Dec 2025	1.0	Central Bank of Kuwait	First Release	Central Bank of Kuwait

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 and financial sector as critical national infrastructure. Accordingly, the Central Bank of Kuwait (CBK) identifies the need for the banking and financial sector and other CBK regulated entities to improve its resilience to cyber-attacks and is undertaking multiple initiatives under the ambit of Cyber and Operational Resilience Framework (CORF). The CORF aims to integrate cybersecurity and cyber resilience within the governance and operations of the Regulated Entities.

This document specifies the 'Cyber Resilience Baselines' (hereinafter referred to as 'Baselines') that the Regulated Entities shall implement to improve their overall cyber posture. This document forms a part of CBK's initiative of Cyber and Operational Resilience Framework for the Kuwaiti Banking and Financial Sector and CBK Regulated Entities.

The Baselines are developed to ensure existence of consistent cybersecurity controls within Regulated Entities and improve the banking and financial sector's and other CBK regulated entities 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 Cyber Resilience 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 covering:

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 apply to all Regulated Entities supervised by the CBK, with compliance to Baselines is subject to CBK's supervision/ assessment.

The applicability extends to the Regulated Entities' employees, third-party vendors, and third-party vendor staff engaged in providing services to the Entity.

To ensure continued compliance, Regulated Entities may seek specific clarifications or approvals from CBK, where necessary.

1.3 Target Audience

The Baselines are issued for the Board of Directors, Executive/Senior Management, information security professionals, 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 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) **Statement of Applicability (SoA)**: Regulated Entities shall complete the SoA to demonstrate the applicability of the CORF domains and sub-domains in relation to the Entity's business model and services provided, where any exclusions shall be formally justified. The SoA shall be submitted ahead of any CORF assessment or audit; and
c) **Periodic / ad-hoc assessment and reporting:** Regulated Entities shall conduct periodic / ad-hoc inherent risk profiling and baselines assessments as stipulated by the 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 Cyber Resilience Baselines

The Cyber Resilience Baselines are established based on the below principles1:

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. Baselines Structure

The Cyber Resilience Baselines are structured as domains, sub-domains, control areas, and controls as defined below:

- the domain specifies the intent for a given area;
- the sub-domain establishes the objective;
- the control area groups related controls within the sub-domain, providing structured focus on specific aspects of the objective; and
- controls specify applicable baselines that shall be covered under each sub-domain and control area.

Structure:

X. (Domain)
X.1 (Sub-Domain)
X.1.1 (Control Area)
X.1.1.1 (Control)

Example:

4. Governance, Risk, and Compliance
4.1 Cybersecurity Governance and Oversight
4.1.1 Board of Directors
4.1.1.1 The Board of Directors (hereinafter referred as, the Board) of Regulated Entities shall……

3.1 Domains

The Cyber Resilience Baselines have been logically grouped into (6) broad domains and (33) 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 Cyber and Operational Resilience Framework (CORF). The identified domains of the Baselines are:

a) **Governance, Risk, 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 Risk Management and Supply Chain Management:** 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) **Emerging Technologies:** This domain defines the controls and security considerations for emerging technologies such as Artificial Intelligence (AI), machine learning, blockchain, and cloud computing. This shall help Regulated Entities to identify, mitigate and effectively manage risks related to emerging technologies.

e) **Payments Security:** This domain defines the baselines that shall be implemented by the Regulated Entities to identify, mitigate and monitor cybersecurity risks related to payment systems.

f) **Operational Resilience:** This domain outlines the controls related to business continuity, disaster recovery and crisis management including the requirements for developing, maintaining, and effectively monitoring cyber resilience efforts. This will help Regulated Entities identify and effectively manage risks related to cyber resilience.

3.2 Sub-Domains

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

Governance, Risk, and Compliance	Technology and Operations		Third-Party Risk Management and Supply Chain Management	Emerging Technologies	Payments Security	Operational Resilience
Cyber Resilience Governance and Oversight	Security Architecture Design	Logging, Monitoring, and Security Incident Management	Third-Party Risk Management (TPRM)	Advanced Technologies Security	Common Security Controls for Electronic Payment Systems	Business Continuity and Disaster Recovery (BC and DR)
Cybersecurity Risk Management	Asset Management	Cybersecurity Testing and Threat Management	Supply Chain Management	Cloud Security	Electronic Payment Transactions Monitoring	Cyber Crisis Management
Compliance	Infrastructure and Network Security	Physical and Environmental Security			Digital Banking Security	
Audit	Endpoint and Device Security	Cyber Threat Intelligence			Payment Card Data Security	
Workforce Management	Email Security	Digital Risk Protection			Security of Customer Self-Service Machines	
	Identity and Access Management				Contactless Payment Technology Security	
	Cryptography					
	Application Security and Secure SDLC					
	Change and Release Management					
	Capacity Management					
	Data Protection and Privacy					

Table 1: Domains and Sub-Domains of Cyber Resilience Baselines

4. Governance, Risk, and Compliance

Overview: Governance, Risk, 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 Cyber Resilience Governance and Oversight

Objective: To ensure robust governance and effective operationalization of Cybersecurity initiatives within Regulated Entities, the Regulated Entities shall establish a comprehensive governance model that ingrain cybersecurity into their organizational structure. This model should clearly define roles and responsibilities with respect to cybersecurity, support the development of a cybersecurity strategy that aligns with the Entity's overall business objectives and sectoral requirements, and establish a cyber resilience policy that sets management's intent and approach to managing cyber risks, in line with the principles outlined in the CBK CORF.

4.1.1 Board of Directors

4.1.1.1. The Board of Directors (hereinafter referred as, the Board) of Regulated Entities shall be the approving authority for the cybersecurity strategy, and shall provide authorization for the cyber resilience policy.

4.1.1.2. The Board may delegate certain responsibilities to relevant committees or independent functions, however, the Board shall retain ultimate accountability for the Entity's overall cyber resilience and shall be reviewed at least annually as part of its formal meetings.

4.1.1.3. The Board shall be accountable, including approving cyber risk appetite and tolerance levels, and ensuring strategic oversight of evolving cybersecurity trends and threats.

4.1.1.4. The Board shall ensure the allocation of adequate cybersecurity budget and resources.

4.1.1.5. The Board shall receive regular updates from the Cybersecurity Steering Committee on the overall status of the cybersecurity program, as well as additional updates as needed on emerging threats or significant changes in the risk landscape. Additionally, the Board shall be informed and kept updated on any legal or regulatory implications of cyber risks.

4.1.2 Cybersecurity Steering Committee

4.1.2.1. The Cybersecurity Steering Committee established with the participation of:

a) the head of the Information Security function;
b) executives and Senior Managers from all relevant departments/ functions (i.e.,CxOs, relevant business functions, and compliance);

4.1.2.2. The Cybersecurity Steering Committee shall be chaired by a designated individual with relevant expertise and sufficient cybersecurity knowledge.

4.1.2.3. The committee shall develop a charter that is approved by the Board. The charter shall include, at a minimum:

a) the committee's objective;
b) the committee members; and
c) the frequency and quorum of meetings, with meetings held at least four (4) times a year.

4.1.2.4. The Board may delegate specific cybersecurity-related responsibilities to this Cybersecurity Steering Committee, which shall be established and mandated by the Board. These responsibilities shall be limited to advisory, oversight, and some operational coordination functions. This committee shall not have the authority to approve strategic decisions, such as the cybersecurity strategy or risk appetite.

4.1.2.5. The Cybersecurity Steering Committee shall:

a) review and endorse the cybersecurity strategy and policy;
b) recommend the Entity's cyber risk appetite and oversee the alignment of the cybersecurity program, strategy, and policy with the overall business objectives;
c) review alignment of the cyber risk tolerance levels with the approved cyber risk appetite;
d) monitor the effectiveness of the cybersecurity program, including Key Risk Indicators (KRIs), Key Performance Indicators (KPIs), and resources allocation;
e) oversee cyber incident response readiness, post-incident reviews, and the effectiveness of the awareness program; and
f) stay updated on emerging cyber threats, regulatory changes, and ensure compliance.

4.1.3 Executive/ Senior Management

4.1.3.1. Executive/ Senior Management shall be the approving authority of cyber resilience policy and cybersecurity initiatives supporting the strategy approved by the Board.

4.1.3.2. Executive/ Senior Management, including CEO and other C-level executives, shall support the effective execution of cybersecurity strategy.

4.1.3.3. Executive/ Senior Management shall be responsible for implementing risk management strategies, ensuring active alignment with the approved cyber risk appetite and tolerance levels, and continuously adapting the Entity's cybersecurity posture to evolving trends and threats.

4.1.3.4. Executive/ Senior Management shall allocate proper cybersecurity budget, define, and assign roles and responsibilities with relevant expertise and in alignment with CORF requirements, and continually promote a cybersecurity culture throughout the Regulated Entity.

4.1.3.5. Executive/ Senior Management shall approve the size and resources of the Information Security function.

4.1.3.6. Executive/ Senior Management shall ensure the alignment and implementation of cybersecurity policies and standards, developed by the Information Security function, across all business functions.

4.1.3.7. Executive/ Senior Management shall also ensure proper segregation between information security and IT Operations by assigning appropriate oversight authority to the Information Security Function.

4.1.4 Information Security Function

4.1.4.1. Regulated Entities shall establish an Information Security function independent from Information Technology operations, empowered by the Board, with oversight from the Cybersecurity Steering Committee, and support from Executive/Senior Management. This independent function shall be headed by a designated Information Security professional and shall have necessary skills, knowledge, and competency.

4.1.4.2. The size of the Information Security function shall be determined based on the complexity, nature of business, technology assets, and complexity of operations.

4.1.4.3. The Information Security Function shall have the authority to oversee and provide independent assurance on the management and effectiveness of key operational security activities, including the Security Operations Center (SOC), cyber threat intelligence, vulnerability management, and incident management processes.

4.1.4.4. The head of the Information Security function shall be responsible for defining and reviewing the cybersecurity strategy.

4.1.4.5. The Information Security function shall define the cyber risk tolerance levels based on the approved risk appetite, ensuring alignment with the organizational objectives, regulatory requirements, and operational capabilities.

4.1.4.6. The Information Security function shall set the policies and standards for the governance, implementation, operation, monitoring, and response of cybersecurity controls in alignment with Regulated Entity's strategy, risk appetite, and risk tolerance levels.

4.1.4.7. 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 the compliance with the applicable regulatory guidance and the entity's risk appetite. The Information Security function shall ensure that cybersecurity awareness and training programs are effectively provided/ delivered to all employees, contractors, and relevant third-party vendors.

4.1.4.8. The Information Security function shall update the Cybersecurity Steering Committee, at least quarterly, and whenever there are any changes or emerging risks that require attention, about the overall status of their cybersecurity program.

4.1.5 Cybersecurity Strategy

4.1.5.1. The cybersecurity strategy shall be defined, approved, implemented, and reviewed at least annually, where:

a) the cybersecurity strategy shall undergo a formal and documented review on annual basis.

b) the cybersecurity strategy shall also be subject to change-driven reviews triggered by significant internal or external factors that require revisions. These factors may include, but not limited to:
    i. major changes in the operating environment (e.g., business expansion, merger and acquisitions, technological advancement).
    ii. new or updated regulatory, legal, or sectoral requirements.
    iii. significant shifts in the cyber threats landscape or newly identified risks.

c) the head of the Information Security function of the Regulated Entity shall present and obtain approval on the defined cybersecurity strategy and roadmap from the Board or the corresponding function/ committee as defined in the organization's structure, annually or following any change-driven revisions.

4.1.5.2. Regulated Entity's cybersecurity strategy shall:

a) define the desired cybersecurity maturity level and 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) Details into cyber initiatives / programs / projects that will enable the successful achievement of the desired cybersecurity capabilities;
d) mandate compliance with applicable regulatory, legal and business requirements; and
e) define the thresholds for cyber KPIs and KRIs, along with the hierarchy for reporting.

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

4.1.6 Cyber Resilience Policy

4.1.6.1. The cyber resilience policy shall be defined, approved, implemented, communicated, enforced, and made accessible to all employees, contractors, and relevant third-party vendors.

4.1.6.2. The cyber resilience policy shall be reviewed at least annually or when warranted by changes to current business processes, technology assets, operating environment, or new regulatory requirements.

4.1.6.3. The cyber resilience policy shall:

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

4.1.6.4. Departmental policies from other functions (such as HR, IT, Risk Management, and Procurement) shall align with the cyber resilience policy, with Executive/Senior Management ensuring this alignment.

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

4.1.6.6. Regulated Entities shall ensure that all employees, contractors and relevant third-party vendors are responsible for complying with the organizational cyber resilience policy, as well as related standards and procedures.

4.1.6.7. The cyber resilience policy shall be approved by the Executive/Senior Management and authorized by the Board to ensure alignment with the Entity's overall objectives and the proper management of cyber risks.

4.2 Cybersecurity Risk Management

Objective: To ensure that cyber risks are identified, analyzed, evaluated, tracked, reported and mitigated appropriately, Regulated Entities shall implement a comprehensive cybersecurity risk management process, integrated into the enterprise-wide risk management framework.

4.2.1 Cybersecurity Risk Management Methodology

4.2.1.1. The cybersecurity risk management methodology shall be defined, and implemented by the Information Security function, in collaboration with relevant teams such as IT, Risk Management, Compliance, and Internal Audit. The methodology shall be approved by the Executive/ Senior Management.

4.2.1.2. The cybersecurity risk management methodology shall be reviewed by the Information Security function on annual basis to ensure continued relevance and effectiveness.

4.2.1.3. Information Security function shall regularly communicate the cybersecurity risk management methodology, at least annually, to all relevant business and technology owners, and annually conduct awareness programs to ensure proper understanding and execution of risk assessments and management across the Entity.

4.2.1.4. Cybersecurity risk management shall be integrated and incorporated with the broader enterprise-wide risk management strategy, by ensuring alignment of cybersecurity risk appetite and response measures with those defined and established at the enterprise level.

4.2.1.5. The Regulated Entities shall ensure that:

a) the cybersecurity risk management methodology is based on international best practices, frameworks, and latest standards such as ISO 31000, ISO 27005, ISO 27001, NIST 800-39 and ISF Standard of Good Practice;
b) scope, periodicity, and execution responsibility for risk assessments and management are defined;
c) risk appetite and tolerance levels are specified and determined based on the organizational priorities and objectives; and

d) processes and templates for risk identification, assessment, treatment, and overall monitoring and reporting are specified and documented within a centralized risk register to ensure a unified and comprehensive approach.

4.2.2 Cybersecurity Risk Identification and Assessment

4.2.2.1. 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.

4.2.2.2. The Regulated Entity shall take into account of the following during risk assessment:

a) regulatory and legal requirements as applicable;
b) technology assets and their criticality;
c) connections with external networks;
d) customer delivery channels;
e) application interfaces;
f) threat scenarios and actors (both internal and external);
g) vulnerabilities stemming from governance, processes, design, infrastructure, or human factors; and
h) active threat intelligence sources.

4.2.2.3. The identified cybersecurity risks, including threats, vulnerabilities, and controls, shall be documented in a centralized risk register.

4.2.2.4. Risks shall be evaluated on the basis of severity, impact to business and operations, and likelihood of their occurrence. The actual residual risk value for each identified risk shall be calculated and included in the risk register.

4.2.2.5. The risk assessment outcomes shall be reported to, discussed with, and agreed upon with the respective Business and Technology risk owners within the Regulated Entity. The relevant business owner(s) (i.e., risk owner(s)) within the Regulated Entity shall accept and endorse the risk assessment results, in alignment with the Entity's risk appetite and tolerance levels.

4.2.2.6. 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 or reported by threat intelligence, indicating new or emerging risks;
d) new third-party agreements are signed, taking into consideration the nature and criticality of the service being outsourced, regardless of whether the services are deemed critical or not. All third-party agreements, including non-critical ones, shall be subject to a cybersecurity risk assessment to ensure alignment with the Entity's cybersecurity requirements.

4.2.3 Cybersecurity Risk Treatment and Monitoring

4.2.3.1. Regulated Entities shall ensure that risks documented in the risk register translate into risk treatment plans that correspond to and address the risks identified in the risk register.

4.2.3.2. Risk treatment shall be categorized (e.g., risk acceptance, risk avoidance, risk mitigation, and risk transfer.), tracked, and managed. In case of risk acceptance, avoidance, or transfer, the justification for the chosen treatment shall be documented, approved, and in line with the Regulated Entity's risk management methodology. The documentation should ensure transparency and clarity for decision-makers, ensuring the reasoning for each treatment decision is formally outlined and established.

4.2.3.3. A risk monitoring process shall be implemented to:

a) track compliance with the defined risk treatment plans;
b) ensure effectiveness of risk mitigation controls; and
c) ensure prioritization, effective management, and monitoring of key risks, based on their potential impact and likelihood.

4.2.3.4. The head of Information Security function shall update the Cybersecurity Steering Committee on a quarterly basis regarding the current status of identified risks, treatment plans, and any changes in the risk profile. Additionally, emergent risks shall be flagged and reported promptly, ensuring that adjustments can be made to the risk treatment plans where necessary.

4.2.4 Cyber Insurance

4.2.4.1. Regulated Entities shall document an evaluation of their need for cyber insurance coverage, including rationale for adopting or not adopting such coverage, based on the organizational risk appetite, as a risk transfer mechanism for certain types of cyber risk.

4.2.4.2. Regulated Entities shall ensure in the event of adopting cyber insurance, that any cyber insurance policy adopted provides coverage for a broad range of losses, including, but not limited to, ransomware incidents, cost of data breaches, third-party liabilities.

4.2.4.3. Regulated Entities shall conduct due diligence on chosen cyber insurance policies, to ensure the exclusions and limitations which may impact the insurance payout(s).

4.2.5 Cybersecurity in Project Management

4.2.5.1. Cybersecurity requirements shall be incorporated into the Regulated Entities' project management methodology, to ensure that cybersecurity risks are identified and addressed.

4.2.5.2. The Regulated Entities' project management methodology shall consider that:

a) cybersecurity objectives are included in the project objectives;
b) the cybersecurity function is involved at all stages of the project;
c) a risk assessment is performed at the onset of the project to identify the cybersecurity risks and to ensure that appropriate cybersecurity requirements are addressed either by existing cybersecurity controls or developed to treat the identified risks;
d) cybersecurity risks are documented and tracked in a centralized project risk register;
e) responsibilities for cybersecurity are defined and responsible stakeholders are identified; and
f) a cybersecurity review is performed by an independent internal party or external third-party.

4.3 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.

4.3.1 Regulatory, Statutory, and Standards Compliance

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

a) CBK requirements, instructions, laws, and regulations, including -but not limited to-:
   i. CBK Law 32;
   ii. Law 20/2014, E-Transaction Law;
   iii. CCTV Law No 61/2015;
   iv. E-Crime Law No 60/2015;
   v. Instructions for Regulation of the Electronic payment of Funds;
   vi. Instructions of Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT);
   vii. Open Banking (OB) Framework; and
   viii. Cyber and Operational Resilience Framework for all Local Banks and Financial Institutions; and
   ix. Other relevant requirements, instructions, regulations issued by CBK.
b) Communication and Information Technology Regulatory Authority (CITRA) laws and regulations; and
c) National Cybersecurity Center (NCSC) Decisions.

4.3.1.2. 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) PCI PIN Transaction Security (PCI PTS);
c) PCI Software Security Framework (PCI SSF)
d) EMV (Europay, MasterCard, and VISA) Technical Standard;
e) SWIFT Customer Security Program (SWIFT CSP); and
f) International Organization of Standardization (e.g., ISO 27001, ISO 22301, ISO 31000).

4.3.1.3. Regulated Entities shall obtain and maintain certifications for ISO 27001, ISO 22301 and PCI DSS, complete the attestation for SWIFT Customer Security Controls Framework (SWIFT CSCF), and shall provide attestation of compliance to CBK upon request or at regular intervals in line with the specific requirements of the relevant standards.

4.3.1.4. Regulated Entities shall maintain a compliance register documenting all applicable compliance requirements. Any changes to these requirements shall be identified, assessed, implemented, and appropriately reflected in the register, which shall be reviewed and updated regularly, at least annually.

4.4 Independent Audit

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

4.4.1 Audit Function of Regulated Entity

4.4.1.1. The audit function shall ensure that independent audits are conducted to evaluate the implementation and effectiveness of the Information Security Management System and cybersecurity controls.

4.4.2 Audit Planning and Execution

4.4.2.1. An audit charter, based on generally accepted auditing standards and the cyber and operational resilience 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.

4.4.2.2. An audit plan shall be defined and approved by the Board.

4.4.2.3. Regulated Entities shall ensure that risk areas, defined in this framework, are audited on regular basis, using a risk-based approach to classify risk areas as per internal business requirements and defined methodologies. The classification of risk areas may consider the criticality of assets, the likelihood of threat occurrence, and the potential impact of a compromise or failure:

a) high-risk areas involve critical assets or processes, face frequent or significant threats, and/or would result in severe consequences if compromised. These areas shall be audited at least annually; and
b) medium- and low-risk areas may have lower criticality, fewer threats, and/or less severe impact. These areas shall be audited at least once in two years.

4.4.3 Independent Third-Party Audits

4.4.3.1. Cybersecurity audits to assess compliance against the CBK CORF shall be performed by independent and competent third-party auditor approved by CBK.

4.4.3.2. The third-party auditors shall:

a) possess relevant certifications such as Certified Information Systems Auditor (CISA), ISO 27001 Lead Auditor, Certified Information Security Manager (CISM), Certified Information Systems Security Professional (CISSP), or equivalent qualifications; and
b) have a minimum of five (5) years of experience auditing information security, cyber security, cyber resilience, and/or business continuity in banking and financial institutions (at least one (1) team member of the audit team).

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

4.4.4 Independent Audit Reporting

4.4.4.1. The Board shall be provided with periodic feedback regarding the comprehensiveness and effectiveness of the cyber resilience policy and its implementation. Audit findings, with focus on high-risk areas and corrective actions, shall be reported quarterly.

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

4.5 Workforce Management

Objective: To ensure secure and cyber-aware workforce, Regulated Entities shall integrate information security, cyber security, and cyber resilience considerations into their human resource policies and procedures, and foster a culture of cybersecurity awareness through continuous training and skill development. This approach aims to protect against inappropriate acts of employees, contractors, and third-party personnel, while ensuring the organization maintains the necessary and adequate information security, cyber security, and cyber resilience resources and expertise.

4.5.1 Personnel Security

Regulated Entities shall:

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

4.5.1.2. Ensure that appropriate confidentiality or Non-Disclosure Agreements (NDAs) are signed by the employees, contractors, and third-party vendors before onboarding or engaging in any activities for the Entity.

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

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

4.5.1.5. Ensure that upon termination, all technology and data assets allocated to employees, contractors, and third-party vendors are returned, and all granted access privileges are promptly revoked.

4.5.2 Training and Awareness

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

4.5.2.2. The security awareness and training program shall be conducted upon hire and at least annually, covering topics such as information security policies, information security roles and responsibilities, relevant procedures, latest cybersecurity threats in the banking and financial sector.

4.5.2.3. Customized role-based security trainings shall be conducted at least annually, ensuring relevance to specific job functions and responsibilities.

4.5.2.4. Specialized awareness programs for the Board and Executive/ Senior Management shall be delivered at least annually, to ensure they understand their roles in developing a cybersecurity culture.

4.5.2.5. All employees, contractors, and relevant third-party staff shall formally acknowledge their awareness, understanding, and compliance with cybersecurity policies, at least annually.

4.5.2.6. Regulated Entities shall conduct customer security awareness campaigns, at least quarterly, addressing potential cybersecurity threats and risks, including phishing, brand misuse, and fraud, and promote practices for safe and secure use of financial services. These campaigns shall be delivered through multiple effective communication channels, such as social media platforms, in-app messages, SMS, emails, and other effective channels.

4.5.2.7. Customers shall be encouraged to report phishing emails or phishing websites or unusual behavior observed through appropriate channels identified by the Regulated Entity.

4.5.2.8. Regulated Entities shall assess and monitor the effectiveness of the security awareness and training programs through knowledge assessments and simulated social engineering attacks (e.g., mock phishing attacks/phishing simulations).

4.5.2.9. Regulated Entities shall retain relevant documented information as evidence of all conducted security awareness and training programs, including attendance records and assessment results.

4.5.2.10. Regulated Entities shall continuously review the content of the security awareness and training programs, incorporating feedback from participants and adjustments based on the evolving threat landscape.

4.5.3 Talent Management

4.5.3.1. A comprehensive professional cyber training and certification plan shall be defined, approved, implemented, and reviewed annually. This plan shall identify the professional certifications and training courses that staff employed by Regulated Entities shall pursue in order to continuously develop their cyber skills and capabilities.

4.5.3.2. Regulated Entities shall provide specialist skills-related training for staff in the relevant business functions in line with their job descriptions, such as:

a) key/critical roles within the organization;
b) information security, cyber security, cyber resilience, cyber security operations, cyber risk management, and internal audit staff;
c) staff involved in developing and maintaining information/technology assets; and
d) staff involved in executing risk assessments.

4.5.3.3. Regulated Entities shall conduct systematic workforce planning to identify and document current and future cybersecurity staffing needs, skill gaps, and resource allocation to meet organizational goals.

4.5.3.4. Regulated Entities shall define clear career pathways for information security, cyber security, cyber resilience, cyber operations, cyber risk management, and internal audit roles, including role progression, leadership development opportunities, and mentorship initiatives, to encourage retention and professional growth.

4.5.3.5. Regulated Entities shall implement retention strategies, such as competitive compensation, flexible working arrangements, career advancement opportunities, and employee recognition programs, to maintain skilled workforce.

4.5.3.6. Cross-training and rotational assignments shall be implemented to broaden staff expertise and ensure workforce resilience.

4.5.3.7. Contingency plans for critical roles pertaining to the implementation and monitoring of this framework shall be developed, including knowledge transfer mechanisms and backup personnel for continuity.

4.5.3.8. Metrics shall be established and monitored to assess the effectiveness of talent management programs, including training completion rates, certifications achieved, employee satisfaction scores, and retention statistics. These metrics shall be reported on quarterly basis to Executive/Senior Management to ensure continuous improvement.

4.5.3.9. A comprehensive annual review of talent management programs shall be conducted, including trend analysis, workforce planning recommendations, and evaluation of program effectiveness. The outcomes of this review and recommendations shall be presented to the Board for strategic oversight and to better refine workforce strategies.

4.5.3.10. Regulated Entities shall foster a culture of continuous learning and innovation by providing access to learning platforms, industry conferences, and knowledge-sharing forums to ensure cybersecurity staff remain up-to-date on the evolution of the field of cyber security, cyber resilience, threat landscape, technologies, etc.

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 secure design in line with the overall strategic objectives of the organization and relevant regulatory requirements.

5.1.1 Formalization and Governance

5.1.1.1. Security architecture design shall be defined, approved by relevant stakeholders (such as IT, Information Security, Risk Management, and relevant Business Units) and implemented.

5.1.1.2. Reviews of the security architecture design shall be performed at least annually, and whenever changes to the environment or business requirements arise considering inputs from IT and information security functions, threat intelligence, incident lessons, and vulnerability assessments.

5.1.2 Security Architecture Core Principles

5.1.2.1. The security architecture shall protect the confidentiality, integrity and availability of Regulated Entities information and be designed to:

a) avoid disruption to service and maintain operational continuity;
b) minimize attack surface to reduce exposure to potential threats;
c) implement zero-trust principles, to limit implicit trust between systems and users; and
d) reduce the impact of cybersecurity incidents on the Entity, by enabling effective detection of the adversaries, timely identification of threats, and proactive incident response mechanisms.

5.1.3 Security-by-Design Considerations

5.1.3.1. The security architecture across all environments (e.g., on-premises, cloud, hybrid environments, etc.) shall be based on ‘zero-trust’ and 'secure-by-design' principles, and consider:

a) assuming no implicit trust and verifying all actions based on the identity, context, and identified / associated risk;
b) applying continuous verification of user identity and access, through evaluating user behavior, access patterns and other associated attributes across a variety of environments, e.g., federated cloud environments, on-premises networks, etc.;
c) micro-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;
d) protection of sensitive data at rest, in use and in transit from unauthorized disclosure, alteration, malicious attacks;

e) principles of multi-layer defense in depth security, least privilege and segregation of duties to ensure users only have access to needed resources;
f) logging, monitoring, and reporting requirements to establish continuous verification;
g) limiting internet access from users, systems and devices unless there is a valid business justification / need;
h) business continuity and disaster recovery arrangements; and
i) specific security considerations which are relevant and important to meet business objectives.

5.2 Asset Management

Objective: To ensure information assets of the organization are identified, classified, protected, and securely managed throughout their lifecycle, Regulated Entities shall implement a robust asset management and classification process aligned with organizational objectives and regulatory requirements.

5.2.1 Asset Management Governance

5.2.1.1. Asset management and classification process shall be defined, approved, implemented, monitored, periodically reviewed and updated -at least annually- to secure assets throughout their lifecycle.

5.2.1.2. Reviews shall also be triggered whenever there are changes in the business, technology landscape, regulations, or asset inventory.

5.2.1.3. 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.

5.2.1.4. All assets shall have a designated Business Owner (Asset/Information Owner) responsible for creating and maintaining the inventory.

5.2.1.5. Each IT asset shall have a designated System Owner, acting as the Data Custodian, responsible for maintaining and supporting the assets under their responsibility.

5.2.2 Assets Identification

5.2.2.1. All information and IT assets shall be identified, documented, and maintained in a comprehensive asset inventory list that includes a complete record of all assets, including those owned or leased, located at third-party sites, or operating on the Entity's premises.

5.2.2.2. The asset inventory list shall contain, at a minimum, the asset name, description, owner, custodian, classification, and End-of-life/end-of-support information.

5.2.2.3. Endpoints (e.g., PCs, laptops) shall be included in the asset inventory list, but their classification and criticality shall be determined and managed dynamically based on the user activities and data they handle.

5.2.2.4. The inventory shall track key lifecycle events, such as acquisition, movement, modification, and decommissioning to maintain inventory accuracy.

5.2.2.5. The asset inventory list shall be reviewed and updated at least quarterly, or as needed following a business, technological, or regulatory change, to ensure accuracy and reflect any change in a timely manner.

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

5.2.3 Assets Classification, Labelling, and Handling

5.2.3.1. Assets shall be classified using a risk-based approach in accordance with their value, importance, criticality, and legal or regulatory requirements.

5.2.3.2. Information asset labeling and handling guidelines shall be defined for each asset classification level. These guidelines shall be reviewed and updated at least annually to reflect any changes in classification regulations.

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

5.2.4 Acquisition, Acceptable Use, and Disposal of Assets

5.2.4.1. The acquisition of information assets shall be consistent with the Regulated Entity's procurement process, licensing agreements, and shall comply with the security architecture and policies.

5.2.4.2. A policy for acceptable use of information assets shall be defined, approved, implemented, and reviewed annually. Reviews shall incorporate any business, regulatory, or technological changes.

5.2.4.3. All assets shall be securely disposed when no longer required, in accordance with relevant regulations, industry requirements and standards, contractual agreements, and internal policies of the Regulated Entities.

5.2.4.4. Procedures for the sanitization and destruction of information assets shall be defined, approved, implemented, and reviewed on an annual basis. This shall be in line with information classification and security requirements.

5.2.4.5. 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, crypto-shredding, etc.).

5.2.4.6. Disposal activities shall be documented for compliance and audit purposes.

5.2.5 Detection and Monitoring of Unauthorized Assets

5.2.5.1. A process shall be defined and implemented to detect, prevent, and manage the use of unauthorized, unmanaged or rogue assets. The process shall be reviewed annually and incorporate enhancements based on monitoring results and emerging risks.

5.2.5.2. Monitoring tools and processes shall be utilized to identify unapproved devices or assets connected to the organization's environment.

5.3 Infrastructure and Network Security

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

5.3.1 Security Configuration Standards

5.3.1.1. Security configuration standards shall be defined, approved, implemented, monitored, and reviewed and updated at least annually to ensure they remain effective, relevant, and aligned with evolving threats, covering all technology assets used within the enterprise.

5.3.1.2. 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.

5.3.1.3. 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, including firmware patches for hardware devices;
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, and 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 sessions (e.g., logout, logoff, close the application page, or application timeout) after a predefined period of inactivity and conditions;
k) proactive measures to protect against malicious software, ransomware, data loss, Denial-of-Service (DoS) attacks, advanced threats etc.;
l) synchronizing system clocks with central-clock; and
m) enabling logging and monitoring.

5.3.1.4. Quarterly periodic checks shall be conducted to ensure compliance against security configuration standards, ensuring continuous monitoring.

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

5.3.2 Network Security

5.3.2.1. The network architecture shall be documented, approved, implemented, periodically reviewed at least annually, even if no changes occur, and updated whenever there are significant changes to the architecture take place, such as major deployments or upgrades.

5.3.2.2. Networks shall be protected through appropriate configuration and implementation of security solutions (e.g. router, firewall, Intrusion Prevention System (IPS), Intrusion Detection System (IDS), proxy, Advanced Persistent Threat (APT) protections, email/Internet filtering, Virtual Private Networks (VPNs) etc.) to protect against and detect cyber threats.

5.3.2.3. The network shall be segregated into production, testing, and development zones with distinct established network security policies for each zone, based on its criticality, purpose, and risk exposure.

5.3.2.4. DMZs shall be implemented to host publicly accessible services, limiting inbound traffic to specific IPs, protocols, and ports.

5.3.2.5. All external connections to enterprise's internal network shall be authenticated and encrypted.

5.3.2.6. Logging of network devices shall be enabled to capture changes made to network configurations and security events.

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

5.3.2.8. Network shall be continuously monitored to detect unauthorized or rogue devices connected to the network. Any such devices shall be immediately isolated or deactivated upon detection.

5.3.3 Network Connections and Application Interfaces

5.3.3.1. Security standards for network connections and application interfaces shall be defined, approved, implemented, reviewed at least annually, and updated.

5.3.3.2. 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 the cloud.

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

5.3.3.4. The network connections and application interfaces shall be tested on an annual basis or following a significant change, to ensure compliance with security configuration standards periodically.

5.4 Endpoint and 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.

5.4.1 Portable Device Security

5.4.1.1. A policy for portable device security shall be defined, approved, implemented, monitored, and reviewed periodically on annual basis, and updated.

5.4.1.2. Portable devices shall be permitted to connect to the enterprise network only after necessary authorization and security validation.

5.4.1.3. Regulated Entities portable device policy shall include Acceptable Use Policy (AUP) to define rules for personal and work-related use.

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

5.4.1.5. All portable devices shall be tagged and assigned to a unique employee, contractor, or third-party vendor staff, and their identity shall be logged and tracked in a centralized inventory.

5.4.1.6. All portable devices that are connected to the enterprise network shall be continuously monitored, to detect unauthorized access or malicious behavior.

5.4.1.7. Lost, rooted, and jailbroken devices shall be blocked from accessing enterprise resources.

5.4.1.8. For devices owned by the Regulated Entity, the portable computing devices of terminated or departing employees, contractor, or third-party vendor staff shall be returned, and all data residing on these devices shall be securely erased or backed up as necessary.

5.4.1.9. For devices owned by the employee (i.e., BYOD), the data of the Regulated Entity residing on these portable computing devices shall be securely backed up and stored in the Entity's systems or secure repositories, and subsequently removed from the employee's device, when no longer required (e.g., upon termination of employment or when storage on the employee's device is no longer necessary).

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

5.4.1.11. 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) endpoint encryption or containerization is implemented for data protection.

5.4.1.12. Regulated Entities shall set a maximum number of devices to be connected to entities network per employee based on business need, to control access and manage risks.

5.4.1.13. All portable devices connected to the enterprise network shall support full disk encryption (e.g., BitLocker for Windows and FileVault for macOS) and pre-boot authentication to prevent unauthorized access.

5.4.1.14. Portable devices shall support remote wipe functionality to allow secure data erasure in case of loss or theft.

5.4.1.15. Portable devices shall be configured with automatic lock and inactivity timeouts after predefined period to prevent unauthorized access.

5.4.1.16. A centralized Mobile Device Management (MDM) platform shall be deployed to monitor and track the usage, configurations, and compliance of all mobile devices connected to the Enterprise network.

5.4.1.17. For employee-owned devices, the Regulated Entity shall implement security controls, including Mobile Device Management (MDM) tools, to enforce policies and prevent data leakage. Corporate data shall be isolated from personal data using containerization or other secure means.

5.4.1.18. Endpoint protection tools (e.g., anti-virus and anti-malware), shall be installed on all portable devices to detect and prevent malicious software.

5.4.1.19. Personal firewalls shall be deployed on all end-user platforms (e.g., Windows, macOS, and mobile devices), with rules aligned with the Entity's network and data protection policies.

5.4.2 Removable Media

5.4.2.1. Procedures shall be implemented to manage removable media in accordance with the information asset classification scheme.

5.4.2.2. By default, usage of removable media shall be blocked, unless a strong business justification is in place and proper approvals for such usage is obtained from Information Security function. All granted exceptions shall be logged and monitored.

5.4.2.3. Removable media shall be securely wiped/sanitized after usage to ensure data is unrecoverable.

5.4.2.4. Removable media shall be inspected in an isolated environment and scanned against malware prior to processing any of its content in the Entity's environment.

5.4.2.5. Media containing sensitive information shall be protected during transportation to prevent unauthorized access, tampering, misuse, or corruption.

5.4.2.6. Backup media and removable media storing classified data shall be encrypted and handled properly as per the defined asset handling guidelines.

5.4.2.7. Removable media that is no longer needed shall be securely disposed and destructed following the Regulated Entity's relevant policies and procedures.

5.5 Email Security

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

5.5.1 Email Usage

5.5.1.1. Email usage guidelines shall be documented, approved, implemented, and reviewed at least annually. The guidelines shall include:

a) granting email access in accordance with access management policy and procedures;
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.

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

5.5.1.3. Employees, contractors, and third-party vendor staff shall use email communication in adherence to data privacy and data security requirements of the regulated entity.

5.5.2 Email Security and Risk Mitigation

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

5.5.2.2. Email filtering and anti-phishing tools shall be deployed to detect and prevent malicious emails.

5.5.2.3. Mechanisms to authenticate email communications and ensure their integrity, reducing phishing risks and preventing email spoofing shall be implemented (e.g., Domain-based Message Authentication, Reporting, and Conformance (DMARC), Sender Policy Framework (SPF), and DomainKeys Identified Mail (DKIM),etc.)

5.5.2.4. Regulated Entities shall implement solutions to monitor, detect, and prevent unauthorized transmission of sensitive data through emails, such as Data Loss Prevention (DLP) solutions.

5.6 Identity and Access Management

Objective: To facilitate secure and appropriate access to systems, services, physical premises, information, and information processing facilities, Regulated Entities shall implement appropriate robust security measures within their access management program, adopting zero-trust principles.

5.6.1 Identity and Access Control Management

5.6.1.1. Access management policy shall be defined, approved, implemented, and reviewed at least annually. The policy shall be based on business and information security requirements and shall leverage the basic cybersecurity principles defined in this document. The policy shall

explicitly reflect zero-trust principles, including identity-based access controls, continuous verification, least privilege enforcement, and strong authentication.

5.6.1.2. 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;
d) dynamic, context-aware access controls based on real-time and risk-based mechanisms; and
e) safe and secure use, management, protection, and disposal of credentials.

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

5.6.1.4. Access and privileges shall be granted to all users strictly on a need-to-know and least privilege basis in line with the access management policy, and after the authorization process is complete.

5.6.1.5. Privileged access shall be granted and managed through a Just-In-Time (JIT) approach, ensuring that privileged rights are provided only when required and for the minimum necessary duration, after the authorization process is complete.

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

5.6.1.7. Unique IDs shall be assigned to each user, system, service, and application, according to a standard naming convention.

5.6.1.8. Generic or Group IDs shall be permitted based on a review and validation of business or operational reasons, and prior approval shall be necessary for creation and usage of such IDs. These Generic and Group IDs shall be reviewed at least twice a year to ensure necessity and proper use. Ownership and accountability of Group IDs shall be formally determined and defined.

5.6.1.9. Authentication information of users shall be stored and transmitted in a secure manner, leveraging proper cryptographic mechanisms.

5.6.1.10. Strong authentication mechanisms, such as passwordless authentication (e.g., device-based authentication) and biometrics, shall be prioritized for critical systems in alignment with zero-trust principles, with continuous verification of user and device trust levels.

5.6.1.11. Concurrent logins shall be monitored and prevented for critical systems and applications, unless explicitly required for operational continuity or due to vendor-imposed technical limitations from the vendor. Any such exceptions shall be handled following the Exceptions Management policy and procedures of the Regulated Entity.

5.6.1.12. Appropriate audit records of all access management activities and user access shall be logged, monitored, and reviewed at least monthly for privileged access and critical systems, with

automated alerts to detect suspicious activities in a timely manner. Broader reviews shall be conducted on quarterly basis for all access logs.

5.6.1.13. Regulated Entities shall conduct access control review at least annually for normal user accounts and quarterly for privileged and third-party vendor accounts, or immediately following any change in personnel, roles, or responsibilities. All inactive accounts and redundant access rights shall be identified and disabled/deleted.

5.6.1.14. Inactive accounts shall be automatically identified after (30) days and disabled after (90) days of inactivity, unless justified and approved through Regulated Entities's documented processes.

5.6.1.15. Users shall activate a password protected screensaver or logoff the application when leaving workstation unattended.

5.6.1.16. Proper identity security solutions, such as Privileged Access Management (PAM) solutions, shall be implemented to manage, monitor, and control privileged access to systems. The solution shall incorporate real-time monitoring and session management controls, ensuring least privilege and continuous verification.

5.6.1.17. Behavioral analytics tools (e.g., User and Entities Behavior Analytics (UEBA)) shall be employed to monitor user activities for anomalies and trigger automated responses to potential security incidents, such as adaptive access restrictions, escalated authentication requirements, or session timeouts.

5.6.2 Remote Access Management

5.6.2.1. The Regulated Entities shall establish, implement, and maintain a remote access policy that defines how remote access is granted, managed, monitored, and secured.

5.6.2.2. All remote access granted to users shall be subject to validation of business or operational reasons, approved by relevant stakeholders after due risk assessment, and limited to a defined time period. Zero trust principles shall be applied while granting remote access.

5.6.2.3. Multi-factor authentication shall be implemented for all remote access users, including contractors and third-party vendors. Additional verification steps (e.g., re-authentication, step-up authentication) shall be required as risk-based access controls, based on dynamic parameters (e.g., the user's location, device health, and unusual behavior), to continuously verify access.

5.6.2.4. Context-aware controls (e.g., device details, behavior analysis, geolocation) shall be leveraged to govern access dynamically based on risk.

5.6.2.5. Entity-owned devices shall be prioritized for remote access usage, with zero-trust principles consistently applied to both entity and personal devices (BYOD).

5.6.2.6. Devices used for remote access shall be patched and up-to-date. Unpatched devices shall be quarantined or remediated.

5.6.2.7. Remote sessions by external third-party vendors shall be time-limited based on business needs, recorded, and monitored.

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

5.6.2.9. Direct remote access to internal production systems shall not be permitted. Access to production environments shall only be allowed through approved mechanisms and controls.

5.6.2.10. All remote access communication and sessions shall be encrypted end-to-end using latest security protocols (e.g., VPN, mTLS).

5.6.2.11. Inactive or idle remote sessions shall be automatically terminated after a defined period. This period shall be determined based on the criticality of the system and exchanged data.

5.6.3 Password Management

5.6.3.1. A comprehensive password management policy shall be documented, approved, implemented and reviewed at least annually or following a significant security incident.

5.6.3.2. The password policy shall include requirements for password history, account lockout, maximum password age, minimum password length, prohibited password lists, and include secure log-on procedures.

5.6.3.3. Passwords shall:

a) be at least twelve (12) or more characters in length;
b) include letters, numbers, and special characters;
c) not contain easily guessable information, such as usernames or birth dates; and
d) be checked against a database of compromised, weak, or commonly used passwords during creation.

5.6.3.4. Multi-Factor Authentication (MFA), such as One-Time Password (OTP), token-based authentication, certificate-based authentication, or biometric methods (e.g., fingerprint or facial recognition), shall be required for all users. Regulated Entities shall prioritize passwordless authentication mechanisms.

5.6.3.5. All systems default, vendor-supplied, and publicly documented accounts passwords (including service accounts) shall be changed prior to deployment and configured to meet the Entities' password policy.

5.6.3.6. Passwords shall be communicated and reset in a secure manner to ensure access by the intended user, with default passwords replaced immediately by the user upon first use.

5.6.3.7. Passwords shall be stored securely using cryptographic hashing algorithms (e.g., PBKDF2) with salting.

5.7 Cryptography

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

5.7.1 Cryptographic Controls and Key Management

5.7.1.1. A cryptographic policy shall be documented, approved, implemented, reviewed on annual basis, and updated. The policy shall include organization specific principles and acceptable use of cryptographic controls and consider industry standards, best practices, and any legal and regulatory requirements.

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

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

5.7.1.3. The key length used for encryption shall be as per the latest globally acceptable industry best practices, and reviewed at least annually for adequacy or whenever vulnerabilities or new recommendations are identified.

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

5.7.1.5. Key-encrypting keys shall be stored separately from data-encrypting keys, and encrypted data sets shall not share the same storage location as their respective encryption keys.

5.7.1.6. Encryption keys shall be reviewed periodically and rotate when suspected of a compromise to limit the data exposure.

5.8 Application Security and Secure SDLC

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.

5.8.1 Secure Software Development Lifecycle (SDLC)

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

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

5.8.1.3. The regulated entity shall ensure that all software, whether developed internally or acquired externally, is accompanied by an up-to-date Software Bill of Materials (SBOM), including those provided by third-party suppliers.

5.8.1.4. Secure design reviews shall be conducted at the architecture and design phases.

5.8.1.5. 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.).

5.8.1.6. A DevSecOps approach shall be followed to integrate security into the development and operations workflows.

5.8.1.7. Secure coding practices shall be adopted as per organizational requirements and global best practices (e.g., Open Worldwide Application Security Project (OWASP) Secure Coding Practices) to ensure common coding vulnerabilities (e.g. Common Weakness Enumeration (CWE) Top 25 Most Dangerous Software Weaknesses list) are addressed during development and appropriate protective, detective, corrective, and recovery control measures are implemented.

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

5.8.1.9. Access to the program source code for in-house developed applications shall be restricted, monitored, and logged. For COTS applications, access to source code shall be governed by storing the code on-premise or strict contractual terms or escrow arrangements.

5.8.1.10. 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.

5.8.1.11. Version control mechanisms shall be employed to track code changes and ensure integrity.

5.8.2 Application Security

5.8.2.1. Either a security assessment certificate or equivalent evidence shall be obtained, or a vulnerability assessment or equivalent testing shall be conducted for COTS products to ensure that the applications are tested and identified vulnerabilities are remediated.

5.8.2.2. All applications, regardless their type, shall undergo comprehensive security assessments, including vulnerability assessments and penetration testing, on periodic basis.

5.8.2.3. 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.

5.8.2.4. Error logs shall be reviewed daily for critical systems and at least monthly for other systems to detect any abnormal behavior and potential attacks.

5.8.3 Application Programming Interface (API) Security

5.8.3.1. APIs shall be designed and developed following secure coding practices (e.g., OWASP API Security Top 10) to prevent vulnerabilities such as broken authentication, data exposure, and lack of rate limiting. Furthermore, disable unused HTTP methods and decommission outdated versions.

5.8.3.2. Regulated Entities shall maintain the inventory of API usage.

5.8.3.3. APIs shall enforce strong authentication mechanisms (e.g., OAuth 2.0, API Keys, mTLS) and implement Role-Based Access Controls (RBAC) to ensure only authorized users and applications can access them.

5.8.3.4. All inputs to APIs shall be validated to prevent injection attacks, and output data shall be properly encoded to mitigate potential risks.

5.8.3.5. Rate limiting and throttling mechanisms shall be implemented to protect APIs against Denial of Service (DoS) attacks and abuse.

5.8.3.6. API traffic shall be encrypted using industry-standard algorithms to ensure the confidentiality and integrity of data in transit.

5.8.3.7. API gateways shall be employed to enforce security policies, manage traffic, and monitor API usage. APIs shall be registered and managed through the gateway to centralize security enforcement.

5.8.3.8. APIs shall undergo security assessments on periodic basis and after major changes, including but not limited to (e.g., functional testing, penetration testing, fuzzing, application security testing (DAST/SAST), runtime testing, and security misconfiguration testing).

5.8.3.9. All API activities, including authentication attempts, data access, and errors, shall be logged and monitored for anomalies and suspicious activities.

5.8.3.10. Regulated Entities shall define and document a lifecycle management process for APIs, including secure deprecation and retirement practices, to prevent vulnerabilities in unused or legacy APIs.

5.8.3.11. APIs shall handle errors securely to avoid exposing sensitive information (e.g., stack traces, database errors) in error responses or messages.

5.8.3.12. For third-party APIs, the Entities shall assess their security posture, ensuring compliance with contractual obligations and industry standards.

5.9 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.

5.9.1 Change and Release Management Process

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

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

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

5.9.1.4. Appropriate documentation, testing, and approvals shall be in place before change is implemented in production. The documentation of the major changes shall include at a minimum:

a) a detailed description of the proposed change;
b) an impact assessment on core business services and customers;
c) risk analysis; and
d) mitigation strategies.

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

5.9.1.6. 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 (as applicable), penetration testing, and vulnerability assessment; and
d) audit trails.

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

5.9.1.8. 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.

5.9.1.9. Regulated Entities shall submit a formal approval request to CBK for any major change in advance of the intended implementation date, following CBK's defined timelines and instructions in this regard. The approval request shall include a detailed description of the proposed change, an impact assessment on core business services and customers, risk analysis, and mitigation strategies. If CBK requested additional information, the Regulated Entity shall respond promptly to ensure timely processing of the request.

5.10 Capacity Management

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

5.10.1 Capacity and Performance Management

5.10.1.1. A capacity management process shall be documented, approved, implemented, and reviewed at least annually.

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

5.10.1.3. The defined thresholds shall be reviewed on quarterly basis or following major incidents, upgrades, or changes to ensure continued relevance and alignment with business needs.

5.10.1.4. Continuous monitoring, measurement, and analysis shall be performed to track asset-level performance, including CPU usage, latencies and response time, storage utilization, throughputs, as well as downtimes and causes of unavailability. Real-time alerts and dashboards shall be utilized to provide early warnings on capacity issues.

5.10.1.5. Regulated Entities shall implement proactive measures to address capacity risks and bottlenecks, by having proper capacity planning ensuring required resources are sufficient to meet current and future business needs in a cost-effective, scalable, and secure manner. Capacity planning shall be conducted on an annual basis and reviewed quarterly and as needed based on changes to business forecasts, infrastructure, or emerging risks.

5.10.1.6. Capacity testing, such as stress testing, shall be performed during system deployments, upgrades, or significant changes to validate resource adequacy.

5.11 Data Protection and Privacy

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

5.11.1 Data Protection

5.11.1.1. A Data Protection policy and supporting procedures for the identification and protection of important records shall be documented, approved, implemented, and reviewed on an annual basis.

5.11.1.2. The policy and procedures shall include specifications for processing, storage, retention and disposal of classified data and information in accordance with:

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

5.11.1.3. Security controls shall be implemented to protect confidentiality, integrity, and availability of classified data and information while at rest, in transit, and during processing or use.

5.11.1.4. Encryption techniques used to protect classified data and information shall be in accordance with the approved cryptography policy of the Regulated Entities, which shall be in line with industry best practices.

5.11.1.5. Data security and privacy measures, including but not limited to access controls, encryption, and monitoring, shall be apply to data shared with supply chain vendors.

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

5.11.2 Data Privacy

5.11.2.1. A data privacy policy shall be documented, approved, implemented, and reviewed annually to align with legal, regulatory, and industry requirements.

5.11.2.2. Regulated Entities shall include privacy-by-design as a core component of the data protection strategy, to ensure that data privacy requirements are embedded into all systems and technologies from the onset of the system / technology life cycle. The following privacy-by-design principles should be taken into consideration:

a) proactive not reactive; Preventative not remedial: Privacy should be integrated into the design from the onset to prevent privacy breaches in a proactive manner.
b) privacy as the default setting: Personal data should be automatically protected in any system without requiring any additional actions to be taken by the concerned users to protect their privacy.
c) privacy embedded into design: Privacy should be a core consideration in system design and architecture.
d) full functionality – Positive-sum, not Zero-sum: Privacy should accommodate all valid interest and objectives without sacrificing elements such as usability, efficiency or functionality.
e) end-to-end security – Lifecycle protection: Data should be protected at all stages of the lifecycle from collection through to deletion, including secure storage, transmission and eventual destruction.
f) visibility and transparency – Keep it open: Systems and processes shall be transparent to ensure authorized users have visibility on how their data is handled.
g) respect for user privacy – Keep it user-centric: The privacy interests of users should be prioritized by the system, including providing user-friendly options to select and manage privacy preferences.

5.11.2.3. The following privacy principles concerning personal data shall be included in the policy:

a) Lawfulness, Fairness, and Transparency: Personal data shall be processed lawfully, fairly, and in a transparent manner in relation to the data subject;
b) Purpose Limitation: Personal data shall be collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archival purposes shall not be considered to be incompatible with the initial purposes;
c) Data Minimization: Personal data collected shall be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed;
d) Accuracy: Personal data shall be 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;
e) Storage Limitation: Personal data shall be 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 if it will be processed solely for archiving purposes to safeguard the rights and freedoms of the data subject. Data retention periods shall be in compliance with CBK relevant instructions, laws, and regulations.;
f) Consent: Personal data shall be collected with explicit consent of the data subject, ensuring that such consent is freely-given, specific, informed, unambiguous and affirmative. Consent should be separate from other terms and conditions and not used as a precondition of signing up to or accessing services, unless necessary for the service itself. Data subjects shall have the ability to withdraw consent at any time;
g) Right to be Forgotten: Data subjects shall have the right to request erasure of their personal data when it is no longer processed, no longer necessary in relation to the original purposes for which it was collected or otherwise processed, consent is withdrawn, or the personal data does not comply with legal and regulatory requirements; and
h) Integrity and Confidentiality: Personal data shall be 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.

5.11.2.4. The Regulated Entities shall promptly notify CBK upon the discovery of a personal data breach, without delay and in accordance with the timelines defined in CBK Operational Resilience Baselines.

5.11.2.5. The Regulated Entities shall notify the data subject in case of a personal data breach, without undue delay, if the breach is likely to result in a high risk to the data subject's rights and freedoms, enabling the data subject to take necessary precautions.

5.11.2.6. A Privacy Impact Assessment (PIA) shall be conducted every two years or whenever significant changes occur in the environment to identify potential personal data at risk and ascertain that appropriate technical measures are in place to protect such information. PIAs shall be reviewed on annual basis.

5.11.2.7. Data protection requirements shall be communicated to, and enforced within outsourcing agreements. The Regulated Entities shall ensure that third-parties adhere strictly to the data privacy and protection requirements and policies.

5.12 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 and maintain appropriate security information and event management program.

5.12.1 Logging and Monitoring

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

5.12.1.2. Logs shall be enabled on all critical technology assets on-premises and in cloud.

5.12.1.3. The granularity level of logging shall be based on the classification of the data and risk assessment. At a minimum, the logs shall contain the following information:

a) user ID (who);
b) timestamp (i.e., date and 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 or settings change access attempts.

5.12.1.4. Relevant log sources and logs received shall be monitored, correlated, and protected against unauthorized tampering.

5.12.1.5. Regulated Entities shall implement adequate technologies, i.e., security information and event management (SIEM) tools, to monitor and log security events, including correlation of events and identification of anomalies and security incidents for further investigation.

5.12.1.6. Automated systems should be used to categorize and prioritize incidents based on the severity of the identified threat, using AI-based risk assessment algorithms.

5.12.2 Detection and Analysis

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

a) Classification and categorization of events and incidents;
b) assigning ownership;
c) assessing whether they constitute security breach;
d) assessing the severity and criticality of the incident; and
e) sharing of incident information and associated threat intelligence.

5.12.2.2. Regulated Entities shall establish and maintain a structured threat hunting process to proactively identify unknown, emerging, or ongoing unresolved threats within the environment.

5.12.2.3. Indicators of Compromise (IoCs) shall be continuously monitored using automated detection techniques and rapidly reported for investigation.

5.12.2.4. 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).

5.12.3 Response and Recovery

5.12.3.1. An Incident Response Team (IRT) or equivalent group shall be formed by Regulated Entities to respond to security incidents. The IRT shall be available 24/7 to respond to information security incidents or events.

5.12.3.2. A documented security incident response plan shall be prepared and made readily accessible to limit or mitigate the impact of security incidents.

5.12.3.3. Incident response playbooks shall be automated to enable timely management and containment of security incidents with minimal human intervention.

5.12.3.4. A summary of incidents shall be reported to Board and Executive/Senior Management on a quarterly basis or more frequently based on the severity and impact of the incident.

5.12.3.5. All reported security incidents shall be tracked, logged, analyzed, and remediated. Remediation strategy shall be implemented in a manner that is consistent with the nature and severity of the incident.

5.12.4 Forensics and Evidence Collection

5.12.4.1. Forensic procedures shall be established, maintained, and reviewed annually to ensure readiness for evidence collection, preservation, and analysis.

5.12.4.2. The forensic procedures shall define roles, responsibilities, and escalation paths to ensure forensic activities are effectively coordinated.

5.12.4.3. The procedures shall mandate and define the appropriate use of forensic tools and techniques to collect, retain, and archive evidence in a way that maintains its integrity for legal or investigative purposes.

5.12.4.4. The procedures shall specify when and how authorization and approval is required from management, law enforcement, or regulator to initiate forensic activities, ensuring compliance with operational, legal, and regulatory mandates.

5.12.4.5. Communication protocols with law enforcement and regulators shall be formally documented in the forensic procedures, including clearly defined Point of Contact (POC), to ensure timely coordination and reporting of incidents, in compliance with confidentiality, privacy, and regulatory requirements.

5.12.4.6. Regulated Entities shall ensure that the personnel involved in forensic investigations are trained and certified in relevant forensic tools and techniques.

5.12.4.7. Chain of custody shall be maintained for all evidence collected, with documented transfers, dates, and individuals involved.

5.12.4.8. Evidence shall be protected with Cryptographic Hash Functions (CHF) (e.g., SHA-256, SHA-512) to ensure it is not tampered. Verification of integrity shall take a place before and after any forensic task.

5.12.4.9. Every forensic task shall be logged and documented, including at a minimum:

a) tools and techniques used, with version numbers and configurations;
b) time-stamped activities from the start to the conclusion of each forensic task; and
c) observations or anomalies detected during the investigation.

5.12.4.10. Regulated Entities shall establish Digital Forensics and Incident Response (DFIR) capabilities through either establishing internal 24/7 cyber incident responders or external cyber incident response retainers such as forensic experts or forensic service providers, to enable smooth cooperation during investigations. DFIR shall include:

a) define roles, responsibilities, scope of collaboration, confidentiality obligations, data sharing protocols, and timelines for joint activities;
b) ensure compliance with legal, regulatory, and privacy requirements, especially for cross-boarder investigations; and
c) Service Level Agreements (SLAs).

5.13 Cybersecurity Testing and Threat Management

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

5.13.1 Vulnerability Management

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

5.13.1.2. 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.

5.13.1.3. Timelines or matrices for addressing vulnerabilities shall be defined based on the type of test conducted, criticality of the asset, severity of the vulnerability, and associated risk level.

5.13.1.4. Regulated Entities shall receive notifications from external threat intelligence feeds and other trusted information sources about latest vulnerabilities. The Entities shall follow a

formal risk-based approach for prioritizing and treating the vulnerabilities identified and notifications received in line with the risk management process.

5.13.1.5. Regulated Entities shall conduct validation after remediating the vulnerabilities to assess and confirm whether the gaps addressed are in line with documented risk mitigation decisions.

5.13.1.6. Regulated Entities shall use external attack surface management to discover, monitor and address vulnerabilities within the public facing assets.

5.13.1.7. The findings of vulnerability assessments shall be documented and reported for initiating remediation activities and tracked till closure.

5.13.1.8. The information security function shall update the Board and Executive/Senior Management on quarterly basis or more frequently, as required, about the effectiveness of vulnerability management process, including key metrics and unresolved issues.

5.13.2 Security Patch Management

5.13.2.1. Security patch management process shall be defined, approved, implemented, and reviewed annually. The effectiveness of the process shall be continuously monitored and measured using relevant metrics (e.g., patching timelines, coverage).

5.13.2.2. Regulated Entities shall define a risk-based patching schedule (e.g. monthly, quarterly, etc.,) based on both the criticality of the asset and the severity of the vulnerability.

5.13.2.3. Emergency patches shall be deployed immediately within an escalated timeframe to address actively exploited vulnerabilities.

5.13.2.4. Exceptions or delays in patch deployments shall be formally justified, documented, approved by relevant stakeholders, and report to Executive/ Senior Management.

Red Teaming and Adversarial Simulations

5.13.2.5. Red teaming exercises shall simulate real-world adversarial Tactics, Techniques, and Procedures (TTPs) to assess the resilience of critical systems, applications, processes, and people against cyber threats.

5.13.2.6. Threat intelligence shall be incorporated into red teaming exercises to ensure scenarios reflect real-world adversary TTPs and emerging threats.

5.13.2.7. Red teaming exercises shall be conducted at least once a year or as required based on changes to the threat landscape, critical systems, or regulatory requirements. Clear objectives, scope, and success criteria shall be defined for each exercise.

5.13.2.8. Regulated Entities shall engage a dedicated qualified team with specialized expertise to conduct red teaming exercises.

5.13.2.9. Red teaming exercises shall be performed without prior knowledge of other teams such as cyber monitoring, incident response and asset owners to maintain scenario realism.

5.13.2.10. Findings from red teaming exercises, including identified vulnerabilities, gaps, and areas for improvement, shall be documented and reported to Executive/ Senior Management and relevant stakeholders for review and action.

5.13.2.11. Regulated Entities shall define and implement a remediation plan with clear timelines address the identified findings. Progress on remediation actions shall be tracked to closure.

5.14 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.

5.14.1 Physical and Environmental Security Controls

5.14.1.1. Physical and environmental security policy shall be documented, approved, implemented, reviewed annually and updated.

5.14.1.2. 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.

5.14.1.3. An approved list of individuals with authorized physical access to a restricted areas shall be maintained and reviewed on a quarterly basis.

5.14.1.4. All access points shall be controlled to prevent unauthorized entry to restricted or 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.

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

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

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

5.14.1.8. 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 in this document.

5.14.1.9. Restricted or 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.

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

5.14.1.11. The implemented physical and environmental controls shall be appropriately and periodically tested, at least quarterly. Preventive maintenance shall be conducted to ensure performance as per intended purpose and specifications.

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

5.14.2 Connected Devices (IoT/OT) Security

5.14.2.1. IoT/OT networks (e.g., CCTV systems, Building Management Systems (BMS)) shall be segregated from IT networks using proper network segmentation and firewalls to prevent unauthorized access or lateral movement.

5.14.2.2. All IoT/OT devices connected to the network shall be identified, inventoried, and categorized based on their criticality. This inventory shall be reviewed and updated on semi-annual basis or as changes to the network occur.

5.14.2.3. IoT/OT devices and their associated networks shall be subject to security assessments, including quarterly vulnerability assessments and annual penetration testing. More frequent assessments shall be considered for critical systems based on the evolving threat landscape or regulatory requirements.

5.14.2.4. Access to IoT/OT devices shall be restricted to authorized personnel, and logical access controls (e.g., strong password, MFA) shall be implemented. Access logs shall be monitored and reviewed at least monthly to identify any suspicious behavior.

5.15 Cyber Threat Intelligence

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

5.15.1 Cyber Threat Intelligence (CTI) Management

5.15.1.1. A process for identification, analysis, prioritization, sharing and management of cyber threats shall be documented, approved, implemented, and reviewed annually.

5.15.1.2. Intelligence from trusted, identified internal and external sources shall be collected, disseminated promptly to relevant stakeholders, and processed consistently and in a timely manner.

5.15.1.3. Intelligence shall cover tactical, operational, and strategic levels to ensure appropriate actions across different functions within the Regulated Entities.

5.15.1.4. Regulated Entities shall implement a Threat Intelligence Platform (TIP) to aggregate and analyze threat intelligence feeds from multiple sources. The TIP shall:

a) centralize threat intelligence feeds for consistent management and enrichment;

b) provide custom scoring and prioritization based on the relevance of threats to the organization;

The TIP shall be integrated with the relevant cyber detection and response tools (e.g., SIEM, SOAR, EDR) to operationalize intelligence in an effective way. This integration shall:

a) enable automated enrichment of security events with threat intelligence;
b) trigger real-time alerts and playbook-driven responses for high-classified incidents; and
c) correlate threat intelligence with internal alerts for more accurate and effective detection and response.

5.15.2 CTI Collaboration and Continuous Improvement

5.15.2.1. Threat intelligence shall drive proactive risk mitigation activities, such as vulnerability management, patch management, and system hardening.

5.15.2.2. Cyber threats and insights shall be communicated to Executive/ Senior management and relevant stakeholders on a timely and need-to-know basis.

5.15.2.3. 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 documented, monitored, and tracked.

5.15.2.4. Regulated Entities shall review and improve their threat intelligence management capabilities on an ongoing basis, with a focus on lessons learnt from incidents, feedback from read teaming and other testing exercises, and evolving threat landscapes and new intelligence sources.

5.15.2.5. Regulated Entities shall define within the cyber threat intelligence process the requirements to continually with the CBK to:

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

5.16 Digital Risk Protection

Objective: To ensure that the Regulated Entities are protected against digital threats and misuse of their brand and reputation in cyberspace, Regulated Entities shall adopt digital risk protection initiatives.

5.16.1 Digital Risk and Brand Protection

5.16.1.1. A policy for protecting the Entity's online presence shall be defined, approved, implemented, and reviewed annually. This policy shall align with the Regulated Entity's incident management policy and procedures.

5.16.1.2. The policy shall include at a minimum, controls to monitor misuse of the brand, domain names, logos, initiatives 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.

5.16.1.3. Regulated Entities shall establish processes and measures to monitor, identify, escalate, and address incidents of digital brand abuse and misuse across various channels, including websites, social media platforms, mobile app stores, and the deep/dark web. The process shall detect and respond to:

a) brand abuse, misrepresentation, and fraudulent activities (e.g., malicious domains, fake social media accounts impersonating the Entities or key personnel, fake mobile applications, and phishing sites);
b) targeted social engineering or phishing campaigns;
c) web defacement or unauthorized content publication on public-facing systems;
d) fake or misleading information about the organization circulating online; and
e) data leaks or unauthorized disclosures of sensitive information.

5.16.1.4. The Regulated Entities shall use an appropriate brand protection solution to enable continuous monitoring and real-time detection of brand misuse and fraudulent activities across digital channels, facilitating swift response and ensuring proactive mitigation.

5.16.1.5. Collaboration with external parties, such as social media platforms, app stores, and domain registrars shall be established to promptly takedown and remove any fraudulent account, content, website, or applications.

5.16.1.6. All content for public facing systems shall be reviewed and approved by relevant internal functions before being published to ensure consistency with the brand policies and guidelines.

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

6. Third-Party Risk Management and Supply Chain Management

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 and supply chain management.

6.1 Third-Party Risk Management (TPRM)

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 Third-Party Risk Management

6.1.1.1. A Third-Party Risk Management (TPRM) framework shall be defined, approved, communicated, and implemented. The framework and associated policies and processes shall be aligned with CBK requirements outlined in the CBK TPRM Baselines. The framework shall be reviewed by Risk Management, Information Security, and Audit functions of Regulated Entities on periodic basis, at least annually.

6.1.1.2. Regulated Entities shall seek approval from CBK before engaging in any significant Information Technology (IT) related third-party agreements.

6.1.1.3. Proper due diligence shall be conducted during the third-party vendor selection process to assess the vendor's suitability. The due diligence shall cover the following:

a) experience and capability of the third-party vendor;
b) financial strength and stability of the third-party vendor;
c) internal control environment of the third-party vendor (SOC1/2, SSAE16/18 …etc. can be considered);
d) cybersecurity practices of third-party vendor implemented to mitigate risks, such as incident management, data protection, and access controls;
e) BCP and DR arrangements of the third-party vendor; and
f) ability to comply with applicable laws, regulations, and industry standards (Attestation of compliance can be considered).

6.1.1.4. Risk assessments shall be conducted for all IT third-party services as part of the Regulated Entity's Third-Party Risk Management (TPRM) framework and as per the risk management process prior to engagement.

6.1.1.5. Regulated Entities shall have written agreements for all IT related third-party arrangements that include minimum cybersecurity requirements and define the scope and governance of the third-party service. The agreements shall include:

a) scope of services and service level requirements;
b) roles and responsibilities with respect to implementation of security requirements;
c) confidentiality and security of information shared and non-disclosure requirements;

d) operations and risk management requirements;
e) business continuity and crisis management requirements;
f) subcontracting and further outsourcing of services;
g) right to audit and inspect;
h) termination clause; and
i) requirements for notifications and disclosures of cyber incidents, data breach, or any other security events.

6.1.1.6. Regulated Entities shall maintain an accurate and up-to-date register of all third-party agreements.

6.1.1.7. Regulated Entities shall perform assessment of third-party vendors to ensure the adequacy of implemented and to be implemented controls to address necessary security requirements as per the third-party agreement. Such assessments shall be conducted annually for significant outsourcing arrangements and on a similar or less frequent basis for other arrangements, or whenever a change occur to ensure ongoing compliance.

6.1.1.8. Existing third-party agreements that are already in place shall also be subject to risk assessments, and any identified gaps shall be addressed promptly through control updates, process improvements, or contractual amendments.

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

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

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

6.1.1.11. Security requirements within third-party agreements shall be reviewed and updated annually or upon significant changes in services provided by third-party vendors.

6.1.1.12. Regulated Entities shall ensure secure disposal of information assets that were exchanged during the execution of third-party agreement, in compliance with data privacy laws, regulatory requirements, and internal policies.

6.2 Supply Chain Management

Objective: To ensure risks arising throughout the organizational supply chain are sufficiently identified, assessed, and managed, Regulated Entities shall establish robust risk management process and mandate inclusion of relevant security controls as part of its supply chain management process.

6.2.1 Supply Chain Risk Management

6.2.1.1. Regulated Entities shall identify suppliers and dependencies to determine points of failures and integrate supply chain risks into the risk management framework.

6.2.1.2. Regulated Entities shall reduce reliance on single-source suppliers by developing alternative sourcing strategies and establishing backup arrangements to ensure services and business continuity.

6.2.1.3. Regulated Entities shall implement real-time monitoring tools and leverage threat intelligence to detect issues and manage emerging risks across the supply chain in a timely manner.

6.2.1.4. Regulated Entities shall segment suppliers based on their risk level and criticality to apply enhanced controls for high-risk third-party vendors and suppliers.

6.2.1.5. Regulated Entities shall ensure that suppliers extend security requirements and obligations to sub-contractors and fourth parties to maintain consistent security across all tiers of the supply chain.

7. Emerging Technologies

Overview: Given the significant and importance of emerging technologies such as artificial intelligence, cloud computing, machine learning, blockchain and others, it is imperative for organizations to ensure adequate risk management of these technologies. The following section specifies the necessary controls to manage the risks associated to emerging technologies and enable Regulated Entities to appropriately secure systems reliant on emerging technologies.

7.1 Advanced Technologies Security

Objective: To ensure secure and reliable incorporation and use of advanced/emerging technologies, Regulated Entities shall implement relevant security policy and controls during technology adoption. Emerging technologies include but are not limited to technologies / capabilities such as artificial intelligence (AI), machine learning (ML), blockchain, distributed ledger technologies (DLTs), and cloud computing.

7.1.1 General Security Requirements

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

7.1.1.2. Regulated Entities shall seek approval from CBK when adopting new and emerging technologies. Regulated Entities shall submit an approval request to CBK, at least one month prior to go-live, outlining the technologies considered, the application of the technology, the risk assessment results along with the corresponding risk response details, as well as any relevant information to support the adoption of new and emerging technologies.

7.1.1.3. Regulated Entities shall integrate considerations related to emerging technologies into their existing risk management frameworks, by using threat modeling to identify potential vulnerabilities associated with these technologies (i.e., data breaches, DLT vulnerabilities, adversarial AI attacks, etc.).

7.1.1.4. 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.

7.1.1.5. Regulated Entities shall establish secure coding practices to be adopted when developing or implementing systems leveraging the capabilities of emerging technologies (i.e., AI, ML, blockchain, etc.) to ensure security principles are built-in.

7.1.1.6. Regulated Entities shall ensure that sufficient tests are carried to ensure that new technology meets the requirements and addresses the identified risks. This includes but is not limited to:

a) sandbox testing, to simulate potential attacks on applications prior to deployment;
b) periodic internal security testing and vulnerability assessments of systems built on emerging technologies;
c) regular security audits and third-party reviews of applications built on emerging technologies.

7.1.1.7. Regulated Entities shall provide appropriate awareness towards customers regarding the use of emerging technologies within relevant products / services offered by the Regulated Entities.

7.1.2 Artificial Intelligence (AI) and Machine Learning (ML) Security

7.1.2.1. Regulated Entities shall ensure that AI and ML models are protected against tampering, poisoning, or manipulation during their training, validation, and deployment stages.

7.1.2.2. Regulated Entities shall implement adequate defenses against adversarial attacks (e.g., evasion, data poisoning, inference attacks) targeting AI models. Industry best practices such as OWASP Top 10 LLM applications should be utilized to address security issues in AI applications.

7.1.2.3. Regulated Entities shall ensure that data used for training and inference in AI models is protected in compliance with applicable data privacy regulations and governance frameworks.

7.1.2.4. Regulated Entities shall ensure that AI and ML models are explainable and auditable, specifically in cases where AI and ML models are involved in making high-impact decisions (i.e., fraud detection, credit risk scoring, etc.)

7.1.2.5. Regulated Entities shall continuously monitor AI and ML models for drift, reliability, traceability, and performance evaluation, as well as regular audits to ensure compliance with security requirements.

7.1.3 Blockchain and Distributed Ledger Technology (DLT) Security

7.1.3.1. Regulated Entities shall ensure the security of the blockchain network, including consensus mechanisms, node communication and smart contract execution through the use of adequate encryption and secure algorithms.

7.1.3.2. Regulated Entities shall ensure that smart contracts deployed on blockchain networks undergo rigorous security audits to identify vulnerabilities and potential logic flaws.

7.1.3.3. Regulated Entities shall implement secure key management practices for public and private keys utilized in blockchain and DLT systems.

7.1.3.4. Regulated Entities shall ensure data integrity across distributed ledgers, through utilizing means such as hashing and digital signatures.

7.1.3.5. Regulated Entities shall establish adequate governance frameworks defining roles and responsibilities for maintaining blockchain networks.

7.1.4 Other Emerging Technologies (Quantum Computing, 5G, etc.) Security

7.1.4.1. Regulated Entities shall start considering the implications of the threats which will eventually be posed by quantum computing, by starting to adopt quantum-resistant cryptographic algorithms.

7.1.4.2. Regulated Entities shall periodically assess cryptographic practices to ensure resistance to quantum computing capabilities.

7.1.4.3. Regulated Entities shall develop a quantum readiness strategy, prioritizing the transition to quantum-resistant cryptographic algorithms across all systems and processes, while also addressing broader risks posed by quantum computing. The strategy shall include timelines and milestones for cryptographic migration, assessment of critical systems and data at risk, third-party dependencies, and operational preparedness.

7.1.4.4. Regulated Entities shall test and validate quantum-resistant cryptographic algorithms in testing environments to ensure compatibility and performance prior to deployment.

7.1.4.5. Regulated Entities shall assess the risks associated with 5G networks, including focusing on vulnerabilities introduced by the expanded bandwidth, edge computing capabilities and low-latency communications.

7.1.4.6. Regulated Entities shall ensure that data transmitted over 5G networks shall be encrypted using end-to-end encryption protocols, focusing on the confidentiality and integrity of information.

7.2 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.

7.2.1 Cloud Governance

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

7.2.1.2. 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.

7.2.1.3. Regulated Entities shall seek approval from CBK at least one month prior to signing any cloud based outsourcing agreements, regarding the use of infrastructure-as-a-service (IaaS), platform-as-a-service (PaaS), and software-as-a-service (SaaS) products which directly or indirectly interact with systems involving sensitive data (i.e., customer, financial, transactional, legal, etc.). 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.

7.2.1.4. Branches of foreign banks shall also obtain CBK approval if their use of cloud services, whether contracted directly by the local branch or indirectly through the group-level agreements, involves the processing or storage of sensitive data related to the branch and its customers.

7.2.2 Cloud Risk Management

7.2.2.1. 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.

7.2.2.2. 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) business continuity and disaster recovery arrangements;
c) access management and segregation of responsibilities with respect to cloud services;
d) location and data residency;
e) business viability, dispute management and arbitration, reputation, experience, exit strategies and conflict of interest;
f) sub-contractors (chain of contractors) engaged by cloud service providers;
g) limitations to right to audit, right to conduct security assessments and right to inspect (onsite and offsite); and
h) sole service providers risks (multiple agreements with same service provider).

7.2.3 Cloud Providers Oversight and Agreements

7.2.3.1. 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.

7.2.3.2. 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.

7.2.3.3. Regulated Entities shall ensure that cloud service providers use latest industry best practice (ISO 27001:2022, ISO 27017: 2015, ISO 27018:2019, NIST Guidelines for Media Sanitization – NIST 800-88) for permanent erasure of data that has been transferred or is no longer needed. Encryption keys shall be also securely destroyed. 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. Regulated Entities shall ask CSPs to provide Certificate of Destruction (CoD) as a proof of completion and compliance.

7.2.3.4. 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, or alternatively, the right to access independent third-party assessment reports (i.e., SOC1, SOC2, SOC3 reports, etc.);
e) code of conduct and dispute management;
f) incident management, crisis management and breach notification strategies; and
g) secure termination of agreement.

7.2.4 Cloud Security Architecture and Compliance

7.2.4.1. Regulated Entities shall ensure that cloud environments follow a security-first architecture approach, incorporating security principles such as least privilege, defense in depth, and zero trust.

a) All cloud services and infrastructure shall be designed to isolate sensitive data and prevent unauthorized access through network segmentation, encryption, and multi-factor authentication (MFA).
b) Cloud security architecture shall adhere to industry best practices and comply with relevant regulations and standards, such as ISO 27001:2022, NIST 800-53, and GDPR.
c) Any change to the cloud security architecture shall be subject to a formal risk assessment and change management process before deployment.

8. Payments Security

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 this document.

8.1 Common Security Controls for Electronic Payment Systems

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

8.1.1 Policy and Governance

8.1.1.1. A policy for securing electronic payment systems shall be defined, approved by the board and/or executive/senior management, implemented, reviewed at least annually, and updated.

8.1.1.2. The electronic payment systems policy shall include:

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

8.1.1.3. Regulated Entities shall conduct annual and ad-hoc independent security audits of the electronic payment systems in accordance with:

a) the assessment procedures outlined in the Cybersecurity Testing and Threat Management Sub-Domain; and
b) Requirements of industry standards (such as PCI-DSS, EMV) and best practices.

8.1.2 Digital Onboarding

8.1.2.1. Regulated Entities shall implement robust identity verification mechanisms to validate customer identities, including government-issued IDs, biometric authentication, or digital ID systems.

8.1.2.2. Digital onboarding processes shall include mechanisms to validate identity documents by:

a) verifying physical security measures (e.g., watermarks, holograms);
b) comparing data extracted from barcodes and Machine-Readable Zones (MRZ) with Optical Character Recognition (OCR)-extracted data; and
c) cross-validating personal details with authoritative sources (e.g., government databases).

8.1.2.3. Regulated Entities shall deploy a digital onboarding technology which shall support liveness detection mechanisms to verify the presence of a live person during onboarding. To ensure authenticity of the biometric data (e.g., face recognition, fingerprint and live selfie matching) shall be performed in alignment with industry standards and best practices (e.g., NIST Face Recognition Vendor Test (FRVT)).

8.1.2.4. Biometric deduplication mechanisms shall be implemented to ensure that customers can enroll only once, preventing duplicate enrollments.

8.1.2.5. Multi-Factor Authentication (MFA) shall be employed during the onboarding process to secure account creation and prevent unauthorized access, including secure methods such as biometrics, device-based authentication, or FIDO2.

8.1.2.6. Automated document verification systems shall validate uploaded documents (e.g., Civil ID, password, proof of address), ensuring data integrity and accuracy. Verified documents shall be securely stored, encrypted, and retained for compliance with legal and regulatory requirements.

8.1.2.7. Fraud detection and prevention systems leveraging advanced technologies (e.g., AI/ML models) shall be implemented to detect anomalies (e.g., synthetic identities, impersonation), and to minimize False Acceptance Rates (FAR) and False Positive Rates (FPR).

8.1.2.8. Location shall be captured during onboarding to be used for fraud detection and address verification.

8.1.2.9. Device geolocation, meta data elements and health checks shall be utilized during onboarding process, along with risk-based policies (e.g., device compliance, location anomalies, Secure Element ID (SEID), device type, source IP and prior fraud indicators) applied to identify potentially high-risk sign-ups or actions.

8.1.2.10. Red flag mechanisms shall be established for high-risk scenarios (e.g., duplicate document submissions, mismatched IP geolocations).

8.1.2.11. Notifications about onboarding activities (e.g., document submission, account creation) shall be sent in timely manner to customers to confirm legitimacy.

8.1.3 Authentication and Access Management

8.1.3.1. Regulated Entities shall set the maximum of 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.

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

8.1.3.3. All devices used for accessing digital banking services and electronic payment systems shall be continuously verified for compliance with security policies, including OS version, patch levels, and device integrity (e.g., non-jailbroken, unrooted). Devices failing compliance shall have their access dynamically restricted or revoked until remediation is completed and compliance is restored.

8.1.3.4. 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). Verification methods may include verification of a registered mobile number combined with a secure PIN, or voice biometrics.

8.1.3.5. Changes to customer sensitive information (such as mobile number and email address) through ATMs, Mobile Applications, Interactive Voice Response (IVR), or Online Banking shall be performed only after establishing authenticity of the customer using Multi Factor Authentication (MFA). In case of change of mobile number, the second factor for authentication shall be sent to the old number. If the old number is inactive or unavailable, alternative verification methods shall be employed, such as biometric authentication or identity verification using government-issued documents (e.g., Civil ID, passport) conducted in-person or at a branch or authorized self-service machine (e.g., Kiosk, ITM).

8.1.3.6. Regulated Entities shall enforce context-aware device re-authentication during changes to customer sensitive information to verify that the requesting device is authorized and uncompromised. Device re-authentication shall include verification of device health, geolocation, and behavior to detect any anomalies or unauthorized attempts.

8.1.4 Transaction Security

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

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

8.1.4.3. Transaction-related messages and notifications (e.g., transaction validation messages, payment confirmations or rejections, MFA messages, error messages, suspicious activity alerts, reminders or updates on transaction limits, etc.) shall not reveal sensitive details or information of the payment systems (infrastructure or application(s)).

8.1.4.4. 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.

8.1.4.5. 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.

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

8.1.4.7. Effective controls shall be implemented to ensure mitigation of interconnectivity and communication-related risks (e.g., risks include Man-in-the-Middle (MitM) attack, authentication bypass, network sniffing, application-layer attacks, misconfigurations, unauthorized access, etc.).

8.1.4.8. Regulated Entities shall provide appropriate facilities for customers to block their payments cards via self-service options or through customer service centers.

8.2 Electronic Payment Transaction Monitoring

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

8.2.1 E-Payment Transactions Monitoring and Control

8.2.1.1. Regulated Entities shall foster a culture of continuous learning by providing access to learning platforms, industry conferences, and knowledge-sharing forums to ensure cybersecurity staff remain up-to-date with evolving threats and technologies.

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

a) transaction limits (e.g., amount limits, number of transactions per day or session);
b) known and emerging fraud scenarios;
c) abnormal payment patterns in relation to the customer's payment transaction history;
d) customer transaction preferences and behavioral patterns;
e) Geolocation-based risks based on the location of the payer and the payee at the time of the payment transaction;
f) Unusual geographic shifts in IP addresses between consecutive transactions or logins that are unrealistic due to the time between events (i.e., occur within a short time period that makes legitimate physical travel impossible given the geographic distance);
g) multiple failed authorization attempts;
h) velocity checks (i.e., frequency and volume of transactions in a short period);
i) changes to sensitive information of customers (e.g., contact details, linked accounts);
j) changes in device details, including eSIM profiles, detected shortly before high-risk or suspicious transactions;
k) critical data elements provided by third-party wallet providers (e.g., Apple Pay, Google Pay), including tokenized payment data, unique wallet identifiers, device scores, account scores, phone number scores, geolocation data, provisioning and onboarding metadata (e.g., Secure Element ID (SEID), device type, source IP, capture mode);
l) device fingerprinting or recognition techniques to detect suspicious devices; and

m) cross-channel monitoring (e.g., correlation of activities across online banking, mobile banking, and card transactions);
n) Deep/Dark Web monitoring for leaked cards data issued by the Regulated Entity.

8.2.1.3. Unusual or suspicious transactions shall be automatically blocked or flagged for additional verification before processing. Such transactions shall be investigated and reported to customers (if necessary).

8.2.1.4. Regulated Entities shall notify customers through effective communication channels for all transactions performed on their accounts, including rejected transactions. Notifications shall include offline delivery mechanisms (e.g., SMS, phone calls), prioritized for high-risk or time-sensitive transactions or activities (e.g., unusual transactions involving large amounts or abnormal patterns, changes to sensitive customer information, multiple failed login or transaction authorization attempts).

8.2.1.5. Alerts and incident logs related to suspicious transactions shall be handled and managed in accordance with the Regulated Entities internal policies.

8.2.2 Fraud Management

8.2.2.1. Regulated Entities shall establish and implement a risk-based fraud management framework, prioritizing detection and mitigation measures based on transaction type, customer risk profile, and payment channel.

8.2.2.2. Regulated Entities shall deploy fraud detection systems capable of analyzing transactions in real-time to identify and block fraudulent activities before completion.

8.2.2.3. Regulated Entities shall implement automated detection tools using AI or ML models to improve the detection of potential fraud attempts and continuously adapt to evolving risks.

8.2.2.4. Fraud response playbook shall be developed, including defined procedures for managing and handling fraud incidents. These playbooks shall cover examples of fraud scenarios such as account takeover through phishing, SIM-swapping, or eSIM-related fraud (e.g., cloning of eSIM, unauthorized activation); unauthorized payment transactions; social engineering schemes using AI chatbots or spoofed banking applications; digital payment fraud involving Quick Response (QR) code manipulation or fake merchant accounts; synthetic identity fraud involving the use of AI-generated identities; and deepfake-enabled fraud.

8.2.2.5. Fraud playbook shall be reviewed and updated at least annually, or more frequently as new fraud trends or regulatory requirements emerge, to ensure it remains effective and compliant.

8.2.2.6. Fraud risks arising from third-party service providers involved in payment processing, such as gateways and/or aggregators, shall be assessed and mitigated. This shall be part of the Entity's risk assessment process.

8.2.2.7. Regulated Entities shall participate in industry-wide fraud threat intelligence sharing initiatives to remain informed about emerging fraud tactics and strengthen collaborative defenses, and improve sector-wide resilience.

8.3 Digital Banking Security

Objective: To ensure confidentiality, integrity, and availability of digital banking services, Regulated Entities shall implement robust security controls to protect these services and ensure secure transactions.

8.3.1 Online and Mobile Banking Security

8.3.1.1. Online banking systems and mobile banking applications shall be configured to ensure that:

a) user sessions terminate automatically after a maximum of five minutes of inactivity and should be greyed-out or cleared from any sensitive information related to customer account being displayed; and
b) concurrent sessions are disallowed.

8.3.1.2. Validity of One-Time Passwords (OTPs) is restricted to a maximum of two minutes. Regulated Entities shall enforce session revalidation mechanisms to ensure continuous validity of user sessions. Revalidation shall be triggered based on pre-defined intervals, changes in session context (e.g., IP address or geolocation anomalies, unusual session activity), or prolonged inactivity. Revalidation shall involve secure identity verification through MFA, biometrics, or other context-aware measures.

8.3.1.3. Regulated Entities shall establish reliable and effective authentication measures by implementing strong Multi-Factor Authentication (MFA) controls to secure access and out-of-band verification methods to authorize critical actions, such as account activation, financial transactions (e.g., fund transfers, bill payments), and beneficiary addition, using the following:

a) OTP generated by third-party authenticator apps;
b) In-app push notification with biometric or PIN approval (for mobile apps only); or
c) Device-based authorization (e.g., FIDO2) tied to a registered mobile device (for mobile apps only).

8.3.1.4. Regulated Entities may adopt other secure and innovative OTP delivery technologies as they evolve and emerge, subject to prior evaluation and approval by CBK.

8.3.1.5. Regulated Entities shall obtain and document customer consent for their preferred OTP delivery method during the onboarding process or as part of profile updates. Customers shall be provided with the option to review and update their preferences at any time.

8.3.1.6. Online banking platforms shall implement anti-phishing controls to identify and validate the user (e.g., username), verify the authenticity of the application (e.g., pre- logon challenge questions, site key, multi-screen authentication, etc.), and authenticate the user with a password as part of the authentication process.

8.3.1.7. Regulated Entities shall implement controls to prevent installation and block usage of mobile banking applications on jail-broken or rooted devices.

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

8.3.1.9. Regulated Entities shall ensure that the mobile banking application verifies the customer's mobile number and employs device authentication mechanisms, such as device fingerprinting, certificate-based authentication, or other advanced device authentication methods for first-time use of applications.

8.3.1.10. Customers may be allowed to access mobile banking application from a limited number of validated devices, up to three. Regulated Entities may permit an increase in the number of allowed validated devices, up to six, provided that strong risk mitigation controls are in place (e.g., strong authentication mechanisms: MFA, biometric verification), device attestation, continuous monitoring and behavioral analysis, periodic revalidation of all registered devices.

8.3.1.11. Regulated Entities shall enforce periodic revalidation of all registered devices at least every six (6) months for high-risk accounts and annually for other accounts. The revalidation process shall include:

a) Customer confirmation of each registered device through secure channels, such as in-app notifications, OTP-based authentication, or biometric authentication;
b) Device attestation checks to verify the security posture of each device (e.g., non-rooted or -jailbroken status, updated OS, encryption enabled); and
c) Automatic deregistration of devices that fail revalidation or remain unvalidated after a period of (30) days, or are deemed inactive for more than six (6) months. Notifications shall be sent to customers regarding any actions taken on unvalidated devices.

8.3.1.12. Customers shall have an option to deactivate any of the registered devices remotely through either the mobile banking application or online banking platform. Notifications shall be sent to customers for all device-related activities (i.e., new device registrations, validations, and deactivations).

8.3.1.13. The mobile banking application shall provide biometric authentication (e.g., fingerprint or facial recognition) as an option for user login, where supported.

8.3.1.14. Regulated Entities shall conduct periodic security assessments, to identify and remediate vulnerabilities associated with their online banking platforms and mobile banking applications, including vulnerability assessments and penetration testing.

8.3.1.15. The Regulated Entities shall ensure that appropriate procedures and security measures are in place to validate the identity of all users enrolled remotely or through non-face-to-face channels.

8.3.2 Open Banking Security

8.3.2.1. Regulated Entities shall establish robust access control mechanisms to ensure that only authorized third-party providers (TPPs) can access customer data, and that customers have adequate control over the permissions granted to TPPs, in line with CBK Open Banking Framework.

8.3.2.2. Regulated Entities shall ensure that only essential customer data is shared with TPPs, and explicit consent shall be obtained from customers for data sharing.

8.3.2.3. Regulated Entities shall conduct thorough risk assessments of third-party providers (TPPs) prior to granting them access to customer data, to ensure that TPPs meet the required security standards.

8.3.2.4. Regulated Entities shall ensure that open banking Application Programming Interfaces (APIs) are developed, deployed and maintained with sufficient security measures focusing on input validation, secure communications and rate limiting, in line with CBK Open Banking Framework.

8.3.2.5. Regulated Entities shall ensure that real-time monitoring of open banking APIs is implemented, to detect and respond to any unauthorized access or unusual activity.

8.3.2.6. Regulated Entities shall ensure that open banking APIs and related infrastructure are resilient to operational failures, with adequate redundancy measures implemented to maintain service availability.

8.3.2.7. Regulated Entities shall periodically assess the security of open banking APIs, by conducting penetration testing and vulnerability assessments, to identify and mitigate any potential security risks.

8.3.2.8. Regulated Entities shall maintain detailed logs of all API access, consent transactions and data sharing events related to open banking systems. These logs should be sufficiently protected and be periodically reviewed as part of internal audits and regulatory inspections.

8.3.2.9. Regulated Entities shall provide customers with adequate awareness regarding open banking, including guidance on managing permissions and access, as well as recognizing potential fraud.

8.3.3 Digital Wallets Security

8.3.3.1. Digital wallets shall enforce MFA for registration, first—time login, and critical actions, such as adding or modifying a payment method, changing account settings, managing authorized devices linked to the wallet, or making high-risk transactions.

8.3.3.2. Regulated Entities shall verify and register devices to access digital wallets through device-binding, ensuring that wallet access and transactions are restricted to a pre-authorized registered device.

8.3.3.3. Digital wallets shall block usage on jail-broken or rooted devices.

8.3.3.4. Tokenization shall be used for processing and storing payment data.

8.3.3.5. APIs and payment gateways used by digital wallets shall strictly adhere to secure development practices, and shall undergo periodic vulnerability assessments and penetration testing, following the defined intervals.

8.3.3.6. Regulated Entities shall ensure that customers can remotely disable digital wallets or unlink devices from the wallet in case of device theft, loss, or compromise.

8.4 Payment Card Data Security

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

8.4.1 Payment Card Data Protection

8.4.1.1. Regulated Entities shall ensure compliance to applicable regulations, industry standards, and best practices (e.g., PCI-DSS, PCI PTS, PCI SSF, EMV) for protecting payment card information and related systems.

8.4.1.2. Complete card number shall never be part of or included in any communication with the customers.

8.4.1.3. Card PIN generation shall be secured through strong cryptographic processes so as to restrict access to PIN only to the intended recipient.

8.4.1.4. Cardholder data shall be tokenized or encrypted at rest or in transit.

8.5 Security of Customer Self-Service Machines

Objective: To prevent compromise or leakage of customer information through customer self-service machines (ATMs, ITMs, KIOSKs, POSs, XTMs, etc.), Regulated Entities shall implement comprehensive physical, environmental, and logical security measures.

8.5.1 Physical and Environmental Security of Customer Self-Service Machines

8.5.1.1. Regulated Entities shall implement physical security measures to protect customer self-service machines from theft, damage, tampering, etc.

8.5.1.2. Regulated Entities shall implement anti-skimming, tamper detection, and other security measures on Customer Self- Service Machines.

8.5.1.3. Regulated Entities shall undertake physical inspection of Customer Self Service Machines and their locations at least quarterly to verify the effectiveness of implemented security measures, identify security gaps, and ensure compliance.

8.5.2 Transaction and Customer Data Security

8.5.2.1. Customer self-service machines shall authenticate customer transactions using a combination of card (e.g. debit card, credit card, tokenized card, civil ID) and PIN (static or one-time) numbers as applicable.

8.5.2.2. Segregation of duties 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 an inactive state and the process is established for activation.

8.5.2.3. The Regulated Entities shall block the card upon three unsuccessful attempts of PIN usage and promptly notify the customer to prevent potential misuse. Requests for activation of such cards shall be undertaken with enhanced authentication and verification procedures, applying diligence through secure channels.

8.6 Contactless Payment Technology Security

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.

8.6.1 Contactless Payment Security Controls

8.6.1.1. Regulated Entities shall conduct risk assessment to identify risks due to use of NFC-enabled cards, QR-based payments, and other contactless technologies and implement appropriate controls to mitigate identified risks.

8.6.1.2. Regulated Entities shall define and enforce appropriate limits on number and value of NFC transactions. Additional authentication (e.g., PIN, biometric) shall be required for transactions exceeding the defined limits.

8.6.1.3. Regulated Entities shall notify customers through effective communication channels in real-time for transactions performed using contactless technologies.

9. Operational Resilience

Overview: Establishing robust cyber and operational resilience is crucial to ensuring the continuity of business operations in the event of a disaster, and it is vital to ensure that all business risks are assessed and prioritized when developing an organizational resiliency strategy. This section outlines the controls and measures that Regulated Entities should consider when establishing their business continuity and disaster recovery programs, to ensure the risks related to BC and DR are managed.

9.1 Business Continuity and Disaster Recovery (BC and DR)

Objective: To ensure system and data availability during adverse situations and disruptive events, Regulated Entities shall adopt appropriate Business continuity and Disaster Recovery program.

9.1.1 Business Continuity and Disaster Recovery Planning and Management

9.1.1.1. Business Continuity, Disaster Recovery (BC/DR), Business Impact Analysis (BIA), Threat Risk Assessments (TRAs), Recovery processes and plans shall be documented, approved, implemented, reviewed and updated annually or upon significant changes.

9.1.1.2. Business Continuity Plans (BCPs) and Disaster Recovery Plans (DRPs) shall be established for individual business units, and integrated into the overall Entity-wide plans.

9.1.1.3. Regulated Entities shall define the Recovery Time Objectives (RTOs), Recovery Point Objectives (RPOs), and Maximum Tolerable Downtime (MTD) for critical systems and functions.

9.1.1.4. An alternate recovery site shall be identified for restoration of critical systems and business operations. This alternate site shall be geographically separate from the primary site.

9.1.1.5. Required work recovery procedures, recovery manuals, and contact lists (including names and phone numbers of the external service providers and relevant staff) shall be up-to-date and made available at the recovery site. These lists shall be reviewed and updated at least annually or more often as required.

9.1.1.6. Recovery strategies shall be defined and approved, entailing:

a) activities to be performed during various crisis scenarios, including cyber attacks;
b) technology or manual workarounds;
c) roles and responsibilities; and
d) communication channels and protocols for updating concerned stakeholders on an ongoing basis.

9.1.2 Backup and Recovery Management

9.1.2.1. A backup strategy shall be defined, approved, implemented, reviewed and updated annually or upon significant changes. The strategy shall include:

a) backup periodicity;
b) secure storage and disposal mechanisms; and
c) security measures to protect information and backup media, including from cyber incidents.

9.1.2.2. Information shall be backed up per the approved backup strategy, stored and retained according to the applicable regulatory requirements and laws.

9.1.2.3. Backups shall be periodically tested, at least quarterly, for selective critical systems leading to testing backups of all critical systems within one year, for recoverability to ensure integrity and completeness of backed-up data.

9.1.3 Critical Services and Dependencies Management

9.1.3.1. Regulated Entities shall identify and document all critical services and their dependencies, including internal systems, third-party vendors, and supply chain components.

9.1.3.2. Interdependencies among critical services shall be assessed, at least annually, to identify single points of failure and mitigate risks.

9.1.3.3. Third-party service providers supporting critical services shall be subject to annual risk assessments.

9.1.3.4. Service Level Agreements (SLAs) with critical service providers shall include requirements for operational resilience, RTOs, and breach notification.

9.1.3.5. Contingency plans shall be established for critical service failures, including redundancy mechanisms or alternative providers.

9.1.4 Testing and Validation

9.1.4.1. Periodic restoration tests, at least annually, shall be conducted on the backed-up information to validate the effectiveness and completeness of the backups.

9.1.4.2. Regulated Entities shall conduct annual business continuity and disaster recovery exercises and tests (e.g. BCP drill, failovers), to ensure the effectiveness of recovery strategies and operational continuity. All critical systems, core activities and system support, and business users involved in these processes shall be part of these tests.

9.1.4.3. Business continuity and disaster recovery test results and deviations, if any, shall be documented with the appropriate action/mitigation plans. The documented outcomes and action plans shall be signed off by Executive/Senior Management.

9.1.4.4. Tabletop exercises shall be conducted annually to assess the effectiveness of recovery methods, validate scenario readiness, and ensure the practicality of action plans.

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

9.1.4.6. In addition to business continuity and disaster recovery testing, Regulated Entities should also consider establishing a comprehensive operational resilience testing program focusing on the ability of the organization to withstand and recover from cyber incidents, operational disruptions and third-party failures.

9.1.4.7. Regulated Entities shall ensure that the comprehensive operational resilience testing program covers all critical business services and processes, with any interdependencies identified and managed appropriately.

9.1.4.8. Regulated Entities shall ensure to perform scenario-based testing to simulate a wide range of disruption scenarios, including cyber incidents, and the results of these tests should be documented for evaluation and continuous improvement.

9.1.4.9. Regulated Entities shall perform operational resilience testing at minimum annually, or when significant changes in the operating environment occur requiring the operational recovery capabilities to be assessed again.

9.1.4.10. Regulated Entities shall ensure that any critical third parties / vendors are considered in the operational resilience testing program to ensure the recovery capabilities and impact of third-party failures are evaluated.

9.2 Cyber Crisis Management

Objective: To ensure consistent interpretation, preparation, response, and recovery throughout the crisis lifecycle, Regulated Entities shall adopt an appropriate effective crisis management program.

9.2.1 Crisis Management Planning and Governance

9.2.1.1. Regulated Entities shall maintain updated crisis management plans that support their enterprise resilience, including cyber crisis management planning as an integrated component. These plans shall be:

a) approved by the Board or Executive/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).

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

9.2.1.3. Crisis Management Team shall be led by the Crisis Response Lead and comprise 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.

9.2.1.4. Regulated Entities shall ensure that the Crisis Response Lead :

a) holds a senior executive position with the authority to make strategic decisions;
b) have skills and experience to understand the Regulated Entity's operations and to and to be able to manage crisis; and
c) have an appointed deputy in the absence of the lead.

9.2.1.5. A cyber crisis management process shall be documented, approved, tested, reviewed and updated annually or upon significant changes. 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.

9.2.1.6. Regulated Entities shall define a severity impact matrix that is approved by their Board or Executive/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 CBK Operational Resilience Baselines, and Entity's specific defined risk appetite; and
c) specify the appropriate mitigating actions for each impact tier.

9.2.2 Crisis Response and Communication

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

9.2.2.2. 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.

9.2.2.3. 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.

9.2.2.4. Regulated Entities shall report incidents, impacting confidentiality, integrity, and/or availability, regardless whether the root cause is cyber or not, to CBK in accordance with the timelines defined in CBK Operational Resilience Baselines, corresponding to the incident severity rating.

9.2.2.5. Regulated Entities shall update CBK on the situation/progress of the reported incidents in accordance with the timelines defined in CBK Operational Resilience Baselines.

9.2.2.6. Regulated Entities shall report incidents in accordance with the predefined templates and communication channels outlined in CBK Operational Resilience Baselines.

9.2.2.7. Regulated Entities shall identify and escalate incidents that meet the criteria for crisis-level event within the defined timeframe as defined and determined in CBK Operational Resilience Baselines.

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

9.2.3 Training, Testing, and Continuous Improvement

9.2.3.1. Regulated Entities shall adopt a continuous learning model to promote ongoing improvements in future readiness for cyber incidents.

9.2.3.2. Regulated Entities shall provide:

a) regular training, at least annually, 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.

9.2.3.3. 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.

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

10.Exceptions Under the CORF

Any exception or exemption to one or more controls outlined in this Cyber Resilience Baselines requires regulated entity to submit a formally justified exception request, including proposed compensating controls. This request shall be submitted to the Central Bank of Kuwait (CBK) for evaluation and approval before any exception or exemption can be granted.

11.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.
Asset	An asset (tangible or intangible) is any resource or item of value owned or controlled by a Regulated Entity that can be used to achieve its objectives.
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

Term	Definitions
	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. 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	Innovative advancements in their early stages of development or adoption, with potential to significant impact on industries by transforming operations, enhancing security, and reshaping traditional services, enabling new business models, improving efficiency, and providing competitive advantage. Examples include AI, ML, Cloud, Blockchain, IoT, 5G, and quantum computing.
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.

Term	Definitions
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.
Information Asset	Data, information, or knowledge that is valuable to an organization and is stored, processed, or transmitted in any form. This includes electronic data, documents, databases, software, and any other information resources that support business operations and decision-making.
Major Change	Major changes include: a) Implementation of a change having an impact on core business services and/or affecting customers; b) Mergers, demergers, or acquisitions that could affect the Entity's structure and operations; c) Introduction of new technologies that process customers data; or d) Significant alterations or updates to the IT infrastructure that could disrupt banking services delivery.
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";

Term	Definitions
	-- 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; 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	Refers to any electronic device that is portable and have the capability to store, transmit, and/or process data, whether it is owned by the Regulated Entity or employees and are allowed to connect to the Regulated Entities network. Examples include -but not limited to- laptops, mobile devices.
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 Executive/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

Term	Definitions
	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 Third-Party Agreements	A significant third-party agreements refers to any third-party arrangement that in the event of failure impacts the operations, service to customers, data privacy, financial stability, and legal and regulatory compliance. This includes a) Core or critical business functions essential to the Entity's operations and delivery of services to customers; b) Access to or processing of sensitive data, including personal or financial data and information; c) Outsourcing of cybersecurity monitoring and response activities, such as Security Operations Center (SOC), and other similar activities that are critical to the Entity's ability to detect and mitigate threats; d) IT infrastructure hosting, platform and cloud services that support critical systems, databases, and applications; e) Payment processing, transaction management, and other related services essential to the business and customer access to financial services; and f) IAM services or other security operations that manage access and encryption to critical systems and data.
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.

12.Appendix - Glossary

Term	Definition
CBK	Refers to the "Central Bank of Kuwait".
CORF	Refers to the "Cyber and Operational Resilience Framework".
Cyber Lexicon	Lexicon of terms related to cybersecurity and cyber resilience published by Financial Stability Board.
Banking and Financial Sector and Other CBK Regulated Entities	Refers to CBK and all entities that are regulated by CBK including Local Banks, Foreign Banks, Exchange Companies, payment service providers, Open Banking Service Providers, and other regulated Finance Companies.
Kuwaiti banks	Refers to banks that have Kuwaiti promoters including Islamic, Conventional, and specialized banks.
Foreign banks	Foreign Banks in the state of Kuwait that are authorized by CBK.
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 ● E-Payment of Funds Companies ● Credit Information Companies ● Open Banking Service Providers
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 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.
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

Term	Definition
ISO/IEC	International Organization for Standardization/ International Electrotechnical Commission
ISF	Information Security Forum
PCI	Payment Card Industry
CIS	Center for Internet Security

Chapter 5: Operational Resilience Baselines

DOCUMENT CONTROL

Date	Version	Author	Change Reference	Reviewer/ Approver
03 Dec 2025	1.0	Central Bank of Kuwait	First Release	Central Bank of Kuwait

TABLE OF CONTENTS

1. Introduction

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) acknowledges that operational resilience, which refers to a regulated entity's capacity to consistently deliver critical business services even during disruptions, is essential for maintaining banking and financial sector stability and consumer trust. As a result, CBK is introducing this Operational Resilience Baselines to mandate all Regulated Entities to build and sustain strong, comprehensive operational resilience capabilities.

Operational Resilience Baselines' (hereinafter referred to as 'Baselines') have been developed to ensure a consistent level of operational-resilience controls across all Regulated Entities and to strengthen the Kuwaiti Banking and Financial sector's ability to withstand, recover and learn from disruptive events. The Baselines have been designed in line with of CBK's regulations, instructions and guidelines, prevalent international operational resilience standards, best practices.

1.1 Objectives

The objectives of the baselines are to:

- Enhance operational resilience across the Kuwaiti banking and financial sector by setting minimum standards that strengthen the ability of Regulated Entities to prevent, respond to, and recover from operational disruptions.
- Ensure a consistent level of operational resilience across Regulated Entities while strengthening overall resilience within the Kuwaiti banking and financial sector.

1.2 Scope

The scope of the baselines includes the development, implementation, and ongoing enhancement of policies, procedures, and controls designed to safeguard the continuity and resilience of Regulated Entities. These measures aim to ensure that critical business services and operations can withstand and recover from disruptions effectively. The baselines are to be applied across key areas of the Regulated Entities, including:

a) business Services and delivery channels;
b) core infrastructure components;
c) resources and personnel; and
d) internal and external Dependencies.

1.3 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 Entity may seek specific clarifications and/or approvals from CBK to ensure continued compliance.

1.4 Target Audience

The Baselines are issued for the Board of Directors, Executive/Senior Management, Business Continuity professionals and any other personnel who are responsible for establishing, implementing, and ensuring compliance with CBK directives.

2. Structure for Baselines

The Operational Resilience Baselines are structured as domains, sub-domains, control areas, and controls as defined below:

- The domain specifies the intent for a given area;
- The sub-domain establishes the objective;
- The control area groups related controls within the sub-domain, providing structured focus on specific aspects of the objective; and
- The controls specify applicable baselines that shall be covered under each sub-domain and control area.

Structure:

X. (Domain)
X.1 (Sub-Domain)
X.1.1 (Control Area)
X.1.1.1 (Control)

Example:

3. Governance and Oversight
3.1 Operational Resilience Governance Structure and Oversight
3.1.1 Board of Directors
3.1.1.1 The Board of Director…..

2.1 Domains

The Operational Resilience Baselines have been logically grouped into 8 broad domains and 17 sub-domains based on the nature of controls. The controls specified within each domain and sub-domain collectively assist in establishing consistent operational resilience controls within Regulated Entities and achieving the objectives of the Baselines. The identified domains of the Baselines are:

a) **Governance and Oversight:** This domain shall establish a structured governance framework, to ensure accountability and alignment with regulatory requirements. This will help the Regulated Entity oversee the implementation of operational resilience across the organization.

b) **Risk and Threat Assessment:** This domain shall enable the identification, assessment, and evaluation of resilience risks, to support proactive mitigation and informed decision-making. This will help the Regulated Entity apply standardized methodologies to manage and treat risks.

c) **Business Continuity Management:** This domain shall define business continuity strategies and plans, to sustain critical business functions during and after disruptions. This will help the Regulated Entity ensure preparedness for service restoration under various disruption scenarios.

d) **Technology Resilience:** This domain shall define the recovery and restoration mechanisms for critical IT systems and infrastructure, to ensure timely resumption of technology services. This will help the Regulated Entity align technology recovery planning with business requirements.

e) **Third Party Risk Management:** This domain shall address all third-party relationships, including outsourcing, service providers, technology vendors, and other external dependencies. It enables regulated entities to assess, monitor, and manage third-party risks that could impact the continuity of critical services, covering the full lifecycle from onboarding to exit.

f) **Incident and Crisis Management:** This domain shall define structured response processes for managing incidents and crises, to enable timely detection, escalation, and resolution of disruptive events. This will help the Regulated Entity coordinate recovery actions and reduce operational impact.

g) **Cyber Resilience:** This domain shall implement controls that enable the Regulated Entity to recover from cyber incidents and continue critical operations with minimal disruption. This will help the Regulated Entity maintain operational continuity and resilience in the face of evolving cyber threats.

h) Training, Testing and Continuous Improvement: This domain shall establish mechanisms for validation, awareness, and review, to enhance preparedness and embed resilience culture and drive continuous improvement. This will help the Regulated Entity improve resilience capabilities through continuous learning and testing.

2.2 Sub-Domains

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

Governance and Oversight	Risk and Threat Management	Business Continuity Management	Technology Resilience	Third Party Resilience	Incident and Crisis Management	Cyber Resilience	Testing, Training and Continuous Improvement
Operational Resilience Governance Structure and Oversight	Risk Assessment Methodology	Business Impact Analysis	Service Management	*Refer to Domain 5 of CBK Third-Party Risk Management Baselines*	Incident and Crisis Management Governance and planning	Refer to Domain 9 of CBK Cyber Resilience Baselines	Training, Testing and Exercising
Operational Resilience Policy and Strategy	Risk Assessment Process	Recovery Strategies	Backup and Recovery Management		Communication and Escalation		
Compliance	Risk Treatment and Reporting	Business Continuity Plans (BCP)	Technology and Resilience Capabilities				
			Technology Recovery Plans				
			Cyber Recovery Plans				

Table 1: Domains and Sub-Domains of Operational Resilience Baselines

2.3 Approach for Implementation

Regulated Entities shall follow a structured approach, which assists in implementing the controls as specified in the Baselines. This approach includes:

a) **Periodic / ad hoc assessment and reporting:** Regulated Entities shall conduct periodic / ad hoc 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 baseline assessment, plans, exceptions, and exclusions and may conduct necessary inspection.

Regulated Entities are expected to follow a clear and structured approach to implement the Baselines. The approach covers the identification, implementation, maintenance, and continual enhancement of operational resilience controls in line with each Regulated Entity's inherent risk profile and critical-service exposure, the implementation shall follow the phases below:

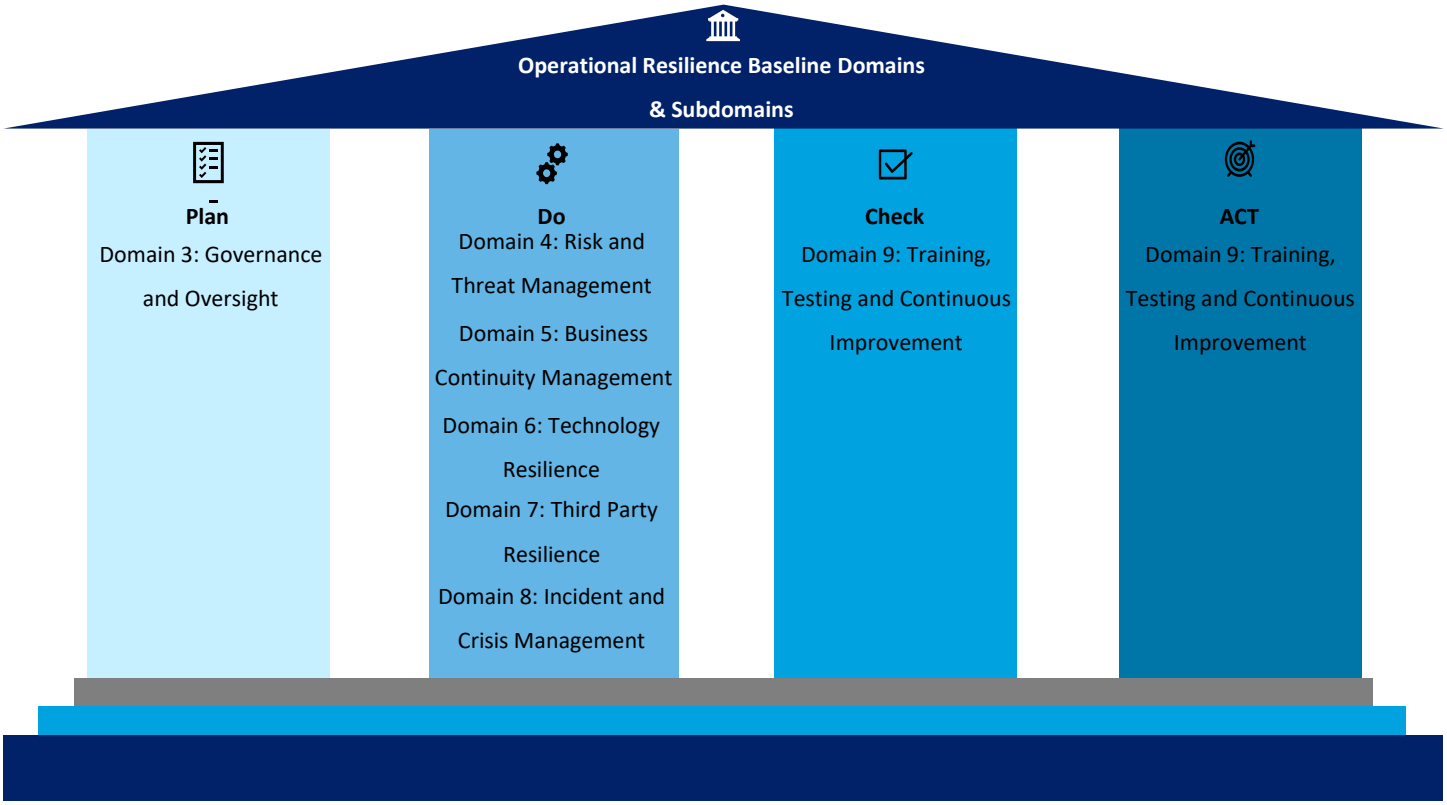


Figure 1: Operational Resilience Baselines Domains

3. Governance and Oversight

Overview: This domain shall establish a structured governance framework, to ensure accountability and alignment with regulatory requirements. This will help oversee the implementation of operational resilience across the regulated entity.

3.1 Operational Resilience Governance Structure and Oversight

Objective: To ensure a clear governance structure for operational resilience. Regulated Entities shall define roles, responsibilities, and oversight mechanisms to ensure accountability and effective execution of resilience activities.

3.1.1 Board of Directors

3.1.1.1. The Board of Directors (hereinafter referred as, the Board), of Regulated Entities shall be the approving authority for the operational resilience strategy and shall provide authorization for the Operational Resilience policy.

3.1.1.2. The Board may delegate certain responsibilities to relevant committees or independent functions, however, the Board shall retain ultimate accountability for the Entity's overall operational resilience and shall be reviewed at least annually as part of its formal meetings.

3.1.1.3. The Board shall be accountable, including approving risk appetite and tolerance levels, and ensuring strategic oversight of evolving operational resilience trends and threats.

3.1.1.4. The Board shall ensure the allocation of adequate budget and resources to execute the required operational resilience activities.

3.1.1.5. The Board shall receive regular updates from the Operational Resilience Steering Committee on the overall status of the baseline, as well as additional updates as needed on emerging threats or significant changes in the threat landscape. Additionally, the Board, shall be informed and kept updated on any legal or regulatory implications of operational risks.

3.1.2 Operational Resilience Steering Committee

3.1.2.1. The Operational Resilience Steering Committee shall be established with the participation of:

a) The head of the Operational Resilience function;
b) Executives and Senior Managers from all relevant departments/ functions (i.e.,CxOs, relevant business functions, and compliance); and

3.1.2.2. The Operational Resilience Steering Committee shall be chaired by a designated senior executive with relevant expertise and sufficient operational resilience knowledge.

3.1.2.3. The committee shall develop a charter that is approved by the Board. The charter must include, at a minimum:

a) The committee's objective;
b) The committee members; and

c) The frequency and quorum of meetings, with meetings held at least four (4) times a year.

3.1.2.4. The Board may delegate specific operational resilience related responsibilities to this Operational Resilience Steering Committee, which shall be established and mandated by the Board. These responsibilities shall be limited to advisory, oversight, and some operational coordination functions. This committee shall not have the authority to approve strategic decisions, such as the operational resilience strategy or risk appetite

3.1.2.5. The Operational Resilience Steering Committee shall:

a) Review and endorse on the Operational Resilience strategy, Operational Resilience policy, Business Impact Analysis, Risk Assessment Consolidation Report, Crisis Management Plan and Recovery Strategy Report;
b) Monitor the effectiveness of operational resilience activities through Key Risk Indicators (KRIs), Key Performance Indicators (KPIs) and resource-allocation status;
c) Recommend the regulated entity's impact-tolerance levels and confirm alignment of those tolerances with overall business objectives and risk appetite;
d) Oversee incident and crisis response readiness, including post-incident reviews, lessons-learned and closure of remediation actions;
e) Oversee testing, exercising, and training plans to ensure they address technology, cyber, supply-chain, and people disruptions, with results used to drive continual improvement; and
f) Stay updated on emerging threats, regulatory changes, and ensure compliance.

3.1.3 Executive/Senior Management

3.1.3.1. Executive/Senior Management shall be the approving authority of operational resilience policy, operational resilience initiatives supporting the strategy approved by the Board, and resilience tolerance levels.

3.1.3.2. Executive/Senior Management, including CEO and other C-level executives, shall support the effective execution of operational resilience strategy.

3.1.3.3. Executive/Senior Management shall be responsible for implementing operational resilience strategies, ensuring active alignment with the approved risk appetite and tolerance levels, and continuously adapting the entity's operational resilience posture to evolving trends and threats.

3.1.3.4. Executive/Senior Management shall allocate proper operational resilience budget, define, and assign roles and responsibilities with relevant expertise and in alignment with ORB requirements, and continually promote a resilience culture throughout the Regulated Entity.

3.1.3.5. Executive/Senior Management shall approve the size and resources of the Operational Resilience function.

3.1.3.6. Executive/Senior Management shall ensure the alignment and implementation of operational resilience policies and standards, developed by the Operational Resilience function, across all business functions.

3.1.4 Operational Resilience Function

3.1.4.1. Regulated Entities shall establish an Operational Resilience Function that is independent of business operations, empowered by the Board, with oversight from the Operational Resilience Steering Committee and in alignment with the Cyber Resilience function. The function shall be headed by a designated Head of Operational Resilience with proven expertise in resilience-related disciplines

3.1.4.2. The size of the Operational Resilience Function shall be determined based on the complexity, nature of business, technology assets, and complexity of operations.

3.1.4.3. The head of the Operational Resilience Function shall be responsible for defining and reviewing the operational resilience strategy.

3.1.4.4. Regulated Entities shall hold the Operational Resilience Function accountable for implementing, maintaining, and coordination of the operational resilience baseline across all relevant domains

3.1.4.5. The Operational Resilience Function shall provide overarching oversight over all functions that support the continuity and recovery of critical business service.

3.1.4.6. The Operational Resilience Function shall be responsible for managing the business continuity activities across the Regulated Entity.

3.1.4.7. The Operational Resilience Function shall ensure that operational resilience awareness and training programs are effectively provided/ delivered to all employees, contractors, and relevant third-party vendors.

3.1.4.8. The Operational Resilience Function shall update the Operational Resilience Steering Committee at least quarterly, or on a need basis, whenever there are any changes or emerging risks that require attention, about the overall status of their program.

3.1.4.9. The Operational Resilience Function shall consolidate the results for the Business Impact Analysis, Technology Impact Analysis, Risk Assessment, Business Continuity Plan, IT Disaster Recovery Plan, incident and crisis management plans and Recovery strategies report and report them to the Executive/Senior Management for approval.

3.2 Operational Resilience Policy and Strategy

Objective: To ensure a structured approach for governing operational resilience. Regulated Entities shall define and maintain an operational resilience policy and strategy aligned with business objectives and regulatory expectations.

3.2.1 Operational Resilience Strategy

3.2.1.1. The operational resilience strategy shall be defined, approved, implemented, and maintained at least annually, where:

a) the operational resilience strategy shall undergo a formal and documented review on annual basis.

b) the operational resilience strategy shall also be subject to change-driven reviews triggered by significant internal or external factors that require revisions. These factors may include, but not limited to:
    i. major changes in the operating environment (e.g., business expansion, merger, technological advancement).
    ii. new or updated regulatory, legal, or sectoral requirements.
    iii. significant shifts in the operational resilience threats landscape or newly identified risks.
c) the head of the Operational Resilience function of the Regulated Entity shall present and obtain approval on the defined operational resilience strategy and roadmap from the Board or the corresponding function/ committee as defined in the organization's structure, annually or following any change-driven revisions

3.2.1.2. Regulated Entities operational resilience strategy shall at a minimum define:

a) The desired operational resilience maturity level and include clear objectives aligned with Regulated Entities business objectives;
b) Road map with timelines for achieving strategic objectives; and
c) Requirements for continual review and validation of alignment of the strategic objectives with operational resilience baselines.

3.2.1.3. Regulated Entities shall identify the responsibility and accountability for strategy implementation and monitoring Operational Resilience Policy.

3.2.1.4. The operational resilience policy shall be defined, approved, implemented, communicated, enforced, and made accessible to all employees, contractors, and relevant third-party vendors.

3.2.1.5. The operational resilience policy shall be reviewed and updated annually or upon significant changes to current business processes, technology assets, operating environment, or new regulatory requirements.

3.2.1.6. Regulated Entities shall develop and maintain an operational resilience policy that:

a) Define operational resilience objectives and scope, Executive/ Senior Management's commitment, operational and resilience roles, and responsibilities, (refer to section 3.2.1) enforcement mechanisms, and deterrents for non-compliance;
b) Incorporate relevant international best practices, frameworks, and standards;
c) Align with the Regulated Entity's business objectives, requirements; and
d) Consider applicable legal, regulatory requirements.

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

3.2.1.8. The operational resilience policy shall be approved by the Executive/Senior Management and authorized by the Board, to ensure alignment with the Entity's overall objectives and the proper management of resilience risks.

3.3 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 operational resilience measures.

3.3.1 Compliance

3.3.1.1. Regulated Entities shall identify, document, and maintain a compliance register documenting all applicable legal, regulatory, and compliance requirements. Any changes to these requirements must be identified, assessed, implemented, and appropriately reflected in the register, which shall be reviewed and updated regularly, at least annually.

3.3.1.2. The compliance register shall cover:

a) CBK requirements, instructions, laws, and regulations, including but not limited to:
   - Operational Resilience Baselines for Kuwaiti Banking and Financial Sector;
   - Cyber Resilience Baselines for Kuwaiti Banking and Financial Sector; and
   - Other requirements, instructions, regulations issued by CBK.

b) Relevant international standards and industry best practices related to operational resilience such as:
   - International Organization of Standardization (e.g., ISO 22301, ISO 31000, and ISO 22361).
   - BCI Good Practice Guideline
   - Basel Committee Principles for Operational Resilience

3.3.1.3. Regulated Entities shall obtain and maintain certification for ISO 22301 and shall provide attestation of compliance to CBK upon request or at regular intervals in line with the specific requirements of the relevant standards.

4. Risk and Threat Management

Overview: This domain shall enable the identification, assessment, and evaluation of business disruption risks and continuous monitoring, to support proactive mitigation and informed decision-making. This will help the Regulated Entity apply standardized methodologies to manage and treat risks.

4.1 Risk Assessment Methodology

Objective: To ensure a structured methodology for assessing business disruption risks. Regulated Entities shall define and implement risk assessment practices to support consistent risk identification, analysis, and treatment across all critical operations and supporting sites.

4.1.1 Risk Assessment Methodology

4.1.1.1. Operational Resilience Function shall define, implement, and maintain a risk assessment methodology on annual basis or upon significant changes to current business processes, technology assets, operating environment, or new regulatory requirements.

4.1.1.2. The Risk assessment shall be part of the regulated entity's overall risk management and aligned with its risk appetite. It shall focus on identifying business disruption risks that could disrupt the regulated entity's operation.

4.1.1.3. Regulated Entities shall ensure that Risk assessment methodology is based on international best practices, frameworks, and standards such as ISO 31000.

4.1.1.4. Operational Resilience Function shall conduct risk assessment for all sites that is used to support the operations of the Regulated Entities, including leased and outsourced sites.

4.2 Risk Assessment Process

Objective: To ensure the identification and evaluation of internal and external threats that could disrupt operations. Regulated Entities shall conduct structured risk assessments to identify relevant risks and assess their potential impact.

4.2.1 Risk Identification and Analysis

4.2.1.1. Regulated Entities shall ensure that the risk identification exercise considers both internal and external threats that could disrupt the regulated entity's operations.

4.2.1.2. Regulated Entities shall consider the following during risk identification:

a) Regulatory and legal requirements as applicable;
b) Environmental threats;
c) Technological threats;
d) Geopolitical threats;
e) Societal threats;
f) Third party threats; and
g) Economic threats.

4.2.1.3. The identified business disruption risks, including threats, vulnerabilities, and controls, shall be documented in a centralized risk register.

4.2.1.4. Risks shall be evaluated based on severity, impact to business and operations, likelihood of their occurrence and controls implemented.

4.3 Risk Treatment and Reporting

Objective: To ensure timely and effective mitigation of identified risks. Regulated Entities shall define and implement appropriate risk treatment plans, monitor their execution, and report the status and effectiveness of treatments to support informed decision-making.

4.3.1 Risk Treatment and Monitoring

4.3.1.1. Regulated Entities shall ensure that risks documented in the risk register translate into risk treatment plans that correspond to and address the risks identified in the risk register.

4.3.1.2. The risk treatment plans shall be reported to, discussed with, and agreed upon with the respective risk owners within the Regulated Entity to provide risk treatment response.

4.3.1.3. Risk treatment response shall be categorized (e.g., risk acceptance, risk avoidance, risk mitigation, and risk transfer.) tracked, and managed.

4.3.1.4. Regulated Entities shall document and approve the justification for risk acceptance, avoidance, or transfer in accordance with their risk management methodology.

4.3.1.5. Regulated Entities shall implement a risk monitoring process to track treatment plan compliance.

4.3.2 Risk Reporting

4.3.2.1. Operational Resilience Function shall consolidate the risk assessment results and report it to the Executive/Senior Management for approval.

4.3.2.2. Operational Resilience Function shall update the Operational Resilience Steering Committee on a quarterly basis regarding the status of identified risks, treatment plans, and any changes in the risk profile.

4.3.2.3. Risk assessment shall be conducted annually or upon significant changes to current business processes, technology assets, operating environment, or new regulatory requirements.

5. Business Continuity Management

Overview: This domain shall define business continuity strategies and plans, to sustain critical business functions during and after disruptions. This will help the Regulated Entity ensure preparedness for service restoration under various disruption scenarios.

5.1 Business Impact Analysis (BIA)

Objective: To ensure identification of critical services, supporting processes, single point of failure (SPOF) across the recovery requirement that may impact recovery. Regulated Entities shall conduct a BIA to assess disruption impacts over time, define recovery objectives, determine required recovery resources, and consolidate interdependencies for effective resilience planning.

5.1.1 BIA Methodology

5.1.1.1. Operational Resilience Function shall define, implement, and maintain a BIA methodology on annual basis or upon significant changes to current business processes, technology assets, operating environment, or new regulatory requirements.

5.1.1.2. Regulated Entities shall ensure that BIA methodology is based on international best practices, frameworks, and standards such as ISO 22301 and BCI Good Practice Guidelines.

5.1.2 Business Processes identification

5.1.2.1. Regulated Entities shall establish and maintain a list of services along with criticality level.

5.1.2.2. Each service shall have a business service owner, who shall be responsible for the outcome and delivery of that service. This individual should have end-to-end accountability for ensuring the resilience and continuity of the service, regardless of functional or geographic boundaries within the regulated entity.

5.1.2.3. Regulated Entities shall perform a BIA to identify and map list of services to their supporting business processes along with the recovery resource requirements.

5.1.3 Recovery Resource Identification

5.1.3.1. Regulated Entities shall identify recovery resources requirement to sustain critical services during disruptions. Identified resource categories shall cover at a minimum building, equipment, technology, human resources, third-party services, and vital records.

5.1.3.2. Regulated Entities shall define the Recovery Time Objectives (RTO) and Recovery Point Objectives (RPOs) for critical systems.

5.1.3.3. Regulated Entities shall identify and map the internal dependencies between each department within the regulated entity.

5.1.4 Identification of Single point of failure and Consolidation

5.1.4.1. Regulated Entities shall identify SPOF across the recovery resource requirements.

5.1.4.2. Operational Resilience Function shall consolidate the BIA results and report it to the Executive/Senior Management for approval.

5.1.4.3. BIA shall be conducted annually or upon significant changes to current business processes, technology assets, operating environment, or new regulatory requirements.

5.2 Recovery Strategies

Objective: To ensure the identification, selection, and implementation of viable recovery strategies for critical services. Regulated Entities shall define appropriate recovery strategies options, allocate necessary resources, and maintain readiness for service restoration.

5.2.1 Recovery Strategy Identification

5.2.1.1. Regulated Entities shall use BIA and Risk Assessment results to formulate recovery strategy options and supporting resource allocation.

5.2.1.2. The recovery strategies shall be formulated based on the identified MAO/MTPD, RTOs and RPOs values of the critical Services/processes and systems.

5.2.1.3. The recovery strategies shall cover the recovery resources requirements (Building, Equipment, Technology, Human Resources, Third Parties and Vital Records) and consider multiple disruption scenarios (i.e. unavailability of the building, unavailability of critical systems etc.).

5.2.1.4. An alternate recovery site shall be identified for restoration of critical systems. This alternate site must be geographically separate from the primary site and not exposed to the same disaster event.

5.2.1.5. Regulated Entities shall identify a recovery strategy for business operations in the event of building unavailability. This strategy may include the use of an alternate site or secure remote working arrangements, as determined by the Regulated Entity.

5.2.2 Recovery Strategy Selection and Monitoring

5.2.2.1. Regulated Entities shall ensure that the selection of recovery strategies is carried out by the Executive/Senior Management considering the cost and benefits of each identified recovery strategy.

5.2.2.2. Regulated Entities shall develop an action plan to implement the selected recovery strategies, including defined activities, responsibilities, and target timelines.

5.2.2.3. Regulated Entities shall track the implementation status of the recovery strategies and solutions.

5.2.2.4. Selected Recovery strategies shall be documented, approved, reviewed, and updated annually or upon significant changes.

5.3 Business Continuity Plans (BCP)

Objective: To ensure the development and maintenance of formal Business Continuity Plans for all critical business functions. Regulated Entities shall define, document, and regularly update BCPs that support timely response, resource coordination, and restoration of essential operations during and after disruptions.

5.3.1 Plan Components

5.3.1.1. Regulated Entities shall define, implement and maintain BCP for each business function on an annual basis or upon significant changes to current business processes, technology assets, operating environment, or new regulatory requirements.

5.3.1.2. The plan shall contain, at a minimum define:

a) Departmental activities (listed in order of priority).
b) Key resources (e.g., Building, Equipment, Technology, Human resources, Third partied and vital records) and internal dependencies;
c) Roles and responsibilities of different stakeholders;
d) Initial response, activation and stand down procedures;
e) Strategy Actions for the selected recovery strategies;
f) A process for relocating to and activating an alternate recovery site for restoration of critical systems and business operations.
g) Guideline for handling media; and
h) A process to resume the regulated entity's operations to business-as-usual once the incident is resolved.

5.3.1.3. Operational Resilience Function shall consolidate the BCP and report it to the Executive /Senior Management for approval.

6. Technology Resilience

Overview: This domain shall define the recovery and restoration mechanisms for critical IT systems and infrastructure, to ensure timely resumption of technology services. This will help the Regulated Entities align technology recovery planning with business requirements.

6.1 Service Management

Objective: To ensure the continuity and resilience of technology services throughout their lifecycle by embedding recovery and support capabilities into service operations. Regulated Entities shall integrate resilience into capacity planning, service-level objectives, and escalation procedures to sustain critical service performance under normal and disrupted conditions.

6.1.1 Service Management

6.1.1.1. Regulated Entities shall maintain a service catalog covering all in-house and outsourced services within the scope of operational resilience, documenting interdependencies and defining KPIs.

6.1.1.2. Regulated Entities shall embed "resilience by design" into the lifecycle of services and support models, ensuring resilience is integrated from planning and development through to operation and decommissioning.

6.1.1.3. Regulated Entities shall conduct periodic service reviews to assess performance and resilience against defined KPIs.

6.1.1.4. Regulated Entities shall define and monitor service-level objectives for recovery and availability.

6.2 Backup and Recovery Management

Objective: To ensure secure and recoverable backup of critical data. Regulated Entities shall implement controls to safeguard data integrity, retention, and availability in alignment with recovery requirements.

6.2.1 Backup Capabilities

6.2.1.1. A backup plan shall be defined, approved, implemented, reviewed, and updated annually or upon significant changes to current business processes, technology assets, operating environment, or new regulatory requirements.

6.2.1.2. The backup plan shall include at a minimum:

a) Backup frequency considering the criticality of data and RPO.
b) Secure storage and disposal mechanisms.
c) Security measures to protect information and backup media, from different types of technology incidents including cyber incidents; and
d) Backup storage in a safe and secure alternate location that is geographically separated from the primary site and not exposed to the same disaster event.

6.2.1.3. Regulated Entities shall implement immutable storage and/or air-gapped backup solutions for critical systems to prevent backup compromise during cyber incidents.

6.2.1.4. Information shall be backed up in accordance with the approved backup plan, stored and retained in alignment with organizational requirements, regulatory requirements and applicable laws.

6.2.1.5. Backups shall be periodically tested, at least quarterly for selective critical systems leading to testing backups of all critical systems within one year, for recoverability to ensure integrity and completeness of backed-up data.

6.3 Technology Resilience Capabilities

Objective: To ensure the continuity and availability of critical operations during technology disruption. Regulated Entities shall design and implement redundancy, high availability, and integrity controls architectures to support uninterrupted operations.

6.3.1 High Availability Design

6.3.1.1. Regulated Entities shall implement high-availability configurations for critical systems identified through the TIA to ensure continuous access and recoverability.

6.3.1.2. Regulated Entities shall adopt scalable and redundant technology architecture to prevent single point of failure.

6.3.1.3. Regulated Entities shall monitor IT system availability and performance periodically.

6.3.1.4. Regulated Entities shall ensure data availability and integrity validation mechanisms.

6.4 Technology Recovery Plans

Objective: To ensure timely restoration of technology services and infrastructure during disruptions, minimizing impact to critical operations. Regulated Entities shall conduct a Technology Impact Analysis (TIA) and establish a documented Disaster Recovery Plan (DRP) to recover IT systems and applications within defined recovery timeframes.

6.4.1 Technology Impact Analysis (TIA)

6.4.1.1. Regulated Entities shall define, implement, and maintain a TIA methodology on annual basis or upon significant changes to current business processes, technology assets, operating environment, or new regulatory requirements.

6.4.1.2. Regulated Entities shall identify the required technology resources to meet the RTO and RPO identified in the BIA.

6.4.1.3. Regulated Entities shall prioritize IT systems based on criticality to support recovery planning.

6.4.1.4. Regulated Entities shall map each IT systems to its underlying infrastructure, including physical/virtual server, operating system, and hardware specifications (e.g., CPU, RAM, storage).

6.4.1.5. Operational Resilience Function shall consolidate the TIA results and report it to the Executive/Senior Management for approval.

6.4.1.6. TIA shall be conducted annually or upon significant changes to current business processes, technology assets, operating environment, or new regulatory requirements.

6.4.2 Recovery Planning

6.4.2.1. Regulated Entities shall define, implement, and maintain an IT Disaster Recovery Plan (IT DRP) to recover and restore technology services and infrastructure components (e.g., data, systems, network, services, and applications), in alignment with the Technology and Business Impact Analysis.

6.4.2.2. The IT DRP shall contain at a minimum to define:

a) Response Team Structure;
b) Role descriptions for the response team;
c) Plan activation and escalation protocols;
d) Recovery steps;
e) Application Recovery interdependency Mapping;
f) IT Recovery Strategies (including cyber-attack recovery);
g) IT environment architecture; and
h) Application Recovery procedures (including cyber-attack recovery).

6.4.2.3. Regulated Entities shall establish a Disaster Recovery (DR) site to enable the restoration of critical technology services in the event of a disruption. The DR site shall be geographically separated from the primary site and equipped with the necessary infrastructure to meet recovery objectives and not exposed to the same disaster.

6.4.2.4. Operational Resilience Function shall report the IT DR Plan to the Executive/Senior Management for approval.

6.4.2.5. Regulated Entities shall review IT DRP annually or when significant changes to current business processes, technology assets, operating environment, or new regulatory requirements.

6.5 Cyber Recovery Plans

Objective: To ensure the timely restoration of technology services and data integrity following cyber incidents. Regulated Entities shall establish documented cyber recovery capabilities to recover from destructive cyber events, including ransomware and malware attacks, while safeguarding the confidentiality, integrity, and availability of critical systems and information.

6.5.1 Cyber Recovery Capabilities

6.5.1.1. Regulated Entities shall identify all, or a subset of critical technology services (Refer to 6.4.1 Technology Impact Assessment) deemed as most critical based on business requirements.

6.5.1.2. Regulated Entities shall establish logically and physically segregated recovery capabilities for technology services identified in section 6.5.1.1, to ensure recovery from cyber incidents impacting primary and disaster recovery sites.

6.5.1.3. Regulated Entities shall validate recovery images, backup integrity, and configuration baselines prior to restoration to ensure recovered systems are free from compromise.

6.5.2 Cyber Recovery Planning

6.5.2.1. Regulated Entities shall define, implement, and maintain a Cyber Recovery Plan (CRP) to restore technology services, applications, and data following a cyber incident.

6.5.2.2. The Cyber Recovery Plan shall include at a minimum:

a) Governance & Scope – Define scope, objectives, roles, responsibilities, assumptions and escalation paths.
b) Recovery Priorities – Identify critical services, dependencies, recovery objectives and priorities.
c) Recovery strategies – Define strategies tailored to cyber-attacks (e.g., ransomware recovery, malware eradication).
d) Recovery Environment – Define recovery environment such as immutable backup, Cyber Vault / Isolated Recovery Environment (IRE), Segregated Network Access, etc.
e) Triggers – Define triggers for invoking the Cyber Recovery Plan (e.g. post containment).
f) Recovery Procedures – Define detailed procedures/technical runbooks for verifying and restoring clean systems and applications.
g) Testing & Validation – Define testing, validation frequency and plan.
h) Continuous Improvement – Define the process for continuous improvement including but not limited to updating the plan post-incident, after major changes and newly identified threats.

6.5.2.3. Regulated Entities shall align the Cyber Recovery Plan with the IT Disaster Recovery Plan (IT DRP), and Business Continuity Plan (BCP), to ensure coordinated recovery.

6.5.2.4. Operational Resilience Function shall submit the Cyber Recovery Plan to the Executive/Senior Management for approval.

6.5.2.5. The Cyber Recovery Plan shall be reviewed annually or upon significant changes to technology assets, cyber threat landscape, or operating environment.

6.5.3 Cyber Recovery Testing

6.5.3.1. Regulated Entities shall conduct cyber recovery testing at least annually, including scenario-based exercises such as ransomware recovery drills, data integrity validation, and reconstitution of compromised environments.

6.5.3.2. Testing results shall be documented, analyzed, and reported to the Executive/Senior Management, with identified gaps remediated within defined timelines.

6.5.3.3. Regulated Entities shall integrate lessons learned from cyber recovery testing into continuous improvement of the Cyber Recovery Plan.

7. Third Party Risk Management

Overview: This domain shall establish requirements for third-party service providers, to maintain continuity of externally delivered critical services. This will help the Regulated Entity assess, monitor, and manage third-party risks.

For further details about Third Party Risk Management controls, Please Refer to Domain 5 of CBK Third-Party Risk Management baselines

8. Incident and Crisis Management

Overview: This domain shall define structured response processes for managing incidents and crises, to enable timely detection, escalation, and resolution of disruptive events. This will help the Regulated Entity coordinate recovery actions and reduce operational impact.

8.1 Incident and Crisis Management Governance and Planning

Objective: To ensure structured and coordinated preparedness for incident and crisis scenarios, the Regulated Entity shall define governance structures, roles, and planning requirements that support timely response, escalation, and recovery while minimizing disruption and regulatory risk.

8.1.1 Response Team

8.1.1.1. Regulated Entities shall define a response structure that comprises of different teams to handle incident and crisis situations (e.g. strategic, tactical, and operational teams) that integrates the technical, business, and management functions of the Regulated Entity.

8.1.1.2. Regulated Entities shall establish a three-layered response structure that includes:

a) Crisis Management Team (Strategic level)
b) Incident Management Team (Tactical Level)
c) Incident Response Team (Operational Level)

8.1.1.3. Regulated Entities shall adopt the severity impact matrix outlined below as its internal impact matrix.

Team Activated	Impact Category / Severity Tier and Impact levels		Operational	Reputational	Theft and data breach	Legal and regulatory
Incident Response Team	Low	**Insignificant**	All service channels are available and no impact on customer base	No negative impact on reputation in social media, local media outlets.	No data breach or theft attempt, and no impact to customers or systems.	No breaches to laws, regulations or contractual obligations
		Low	Few service channels are not available causing minimal disruption and impacting less than xxx% of customers base.	Few social media posts with limited reach (<# views) and no reporting in local media outlets.	Attempted theft or exposure of non-sensitive data with no material loss or customer impact.	Reportable breaches or temporary inability to comply with regulations
Incident Management Team	**Medium**	**Moderate**	# service channels are not available causing noticeable disruption and impacting x%–x% of	Between # to # negative posts from public figures on social media platforms that have	Contained incident involving unauthorized access or minor financial loss, with	Reportable breaches which result in regulatory investigation

			customers base.	a potential of trending with moderate reach (#-# views) due to engaging content, relevant hashtag, tagging of the regulated entity and limited coverage by local media outlets.	limited customer data affected.	and remediation plans with defined timelines
Crisis Management Team	High	**High**	# services channel are not available causing major disruption and impacting x%–x% of customers base.	Between # to # negative posts from public figures on social media platforms that is trending with high engagement (#-# views), cross platform sharing and traction via hashtags and reports in national media.	Confirmed data breach or theft involving sensitive information and multiple affected customers.	Reportable breaches or failures identified by regulatory authorities which result in financial penalties
		Severe	No service channel is available causing operational shutdown and impacting more than x% of customers base.	More than # negative posts from public figures on social media platforms that gained widely viral engagement with a massive reach (>#views), along with headline coverage in major national and international media.	Major data breach or large-scale financial theft with widespread exposure of sensitive data and customer harm.	Formal regulatory intervention, including financial penalties which results in appointment of external 3rd party advisors to oversee or implement remediation plans
***Note:** The impact level shall be determined based on the highest severity observed across one or more impact categories, recognizing that a single significant impact in any category is sufficient to trigger the corresponding severity tier.						

8.1.1.4. Regulated Entities shall establish an Incident Management Team (IMT) that is activated and structured based on the nature, scope, and impact of the incident. The team shall include Incident Responders from the impacted function(s).

8.1.1.5. IMT leader shall be designated to lead response activities, oversee documentation of actions taken, and initiate a post-incident review upon resolution.

8.1.1.6. Regulated Entities shall maintain a Crisis Management Team distinct from Incident Management and Incident Response teams.

8.1.1.7. Crisis Management Team shall be led by the Crisis Response Lead and can comprise empowered representatives from Human Resources, Operations, Information Technology, Information Security, Legal, Finance, Communications, Log keeper and Business Continuity. The team shall:

a) Assess the impacts of the crisis;
b) Maintain centralized and strategic oversight of the crisis;
c) Mobilize and deploy necessary internal and external resources to deliver the response;
d) Oversee execution of response activities;
e) Provide strategic inputs regarding crisis communication with internal and external stakeholders throughout the crisis management life cycle; and
f) Monitor the effect of the crisis and take necessary actions to minimize the financial, operational, reputational and/or legal damages.

8.1.1.8. Regulated Entities shall ensure that the Crisis Response Lead shall:

a) Holds a senior executive position with the authority to make strategic decisions;
b) Have skills and experience to understand the Regulated Entity's operations and to be able to manage the crisis; and
c) Have an appointed deputy in the absence of the lead.

8.1.1.9. Regulated Entities shall have incident and crisis management response toolkit (e.g., a decision and action logging) to create an auditable trail of response considerations and assist in improvements based on lessons learned.

8.1.1.10. Regulated Entities shall establish a crisis command center.

8.1.2 Plans Development

8.1.2.1. Regulated Entities shall document, review, and maintain Incident and crisis management plans that supports their response, including incident and crisis management planning as an integrated component on annual basis. The plan shall be:

a) Approved by the Executive/Senior Management;
b) Implemented at regulated entity wide to ensure coverage of key functions, authorities, and responsibilities;
c) Aligned with legal, regulatory, and organizational requirements; and
d) Aligned with operational risk management considerations (e.g., DR, BC, and communications [internal/external] policies, plans, procedures, and templates).

8.1.2.2. Regulated Entities shall develop and maintain incident management plans that are proportionate with the nature, scale, and complexity of its operations, and shall, at a minimum, include the following components:

a) Team Structure;
b) Role descriptions for the response team;
c) Incident classification criteria and severity levels;

d) Activation and escalation protocols;
e) Incident Lifecycle; and
f) Communication procedures with internal and external stakeholders.

8.1.2.3. Regulated Entities shall develop and maintain crisis management plan that include at a minimum:

a) Criteria for declaring a crisis;
b) Activation and escalation mechanism for crisis response;
c) Crisis Management team structure;
d) Contact details of the crisis management team members and their backups;
e) Crisis response and recovery lifecycle;
f) Set of responsibilities to be undertaken before, during, and after a crisis or disaster; and
g) Communication protocols to address communication with the internal and external stakeholders during a crisis.

8.2 Communication and Escalation

Objective: To ensure timely, coordinated, and accurate communication during incidents and crises, the Regulated Entity shall establish structured escalation protocols and communication procedures to support effective decision-making, stakeholder engagement, and regulatory reporting.

8.2.1 Internal and External Communication

8.2.1.1. Regulated Entities shall have documented communication protocols that pre-define incident and crisis communication statements for various scenarios, communication channels, frequency of communication and responsibilities to ensure that accurate and timely information is disseminated to all internal and external stakeholders.

8.2.1.2. Regulated Entities shall implement effective communication mechanisms to support timely contact with responders and employees in the event of crisis.

8.2.1.3. Regulated Entities shall assign a crisis communication team responsible for managing all communication activities during crisis.

8.2.1.4. Regulated Entities shall appoint a spokesperson responsible for communicating with external stakeholders during the crisis.

8.2.2 Escalation and reporting to CBK

8.2.2.1. Regulated Entities shall initially report incidents to CBK in accordance with the below timelines, corresponding to the incident severity rating:

a) Medium severity incidents shall be reported within (4) hours of discovery; and
b) High severity incidents shall be reported within (1) hour of discovery.

8.2.2.2. Regulated Entities shall update CBK on the situation/progress of the reported incidents in accordance with the below timelines:

a) Medium severity incidents shall be updated on daily basis or when requested by CBK; and

b) High severity incidents shall be updated in every 4 hours from prior notification, or when requested by CBK.

8.2.2.3. Regulated Entities shall submit closure incident report to CBK in accordance with the below timelines, corresponding to the incident severity rating:

a) Low severity incidents shall be consolidated and reported on a monthly basis; and
b) Medium and High severity incidents shall submit closure report once the incident is resolved.

8.2.2.4. Regulated Entities shall determine the estimated financial loss in the initial situational/progress report and confirm the final loss amount in the closure report.

8.2.2.5. Regulated Entities shall report incidents in accordance with the predefined templates (specified in the Appendix section 12.1) and communication channels.

Notification requirements for Regulated Entities to CBK			
Severity	**Initial Reporting**	**Situation Reporting**	**Closure Reporting**
High	Within 1 hours of discovery	Every 4 hours	Upon closure
Medium	Within 4 hours of discovery	Once a day	Upon closure
Low	Not Applicable	Not Applicable	Monthly

9. Cyber Resilience

Overview: This domain shall implement controls that enable the Regulated Entity to recover from cyber incidents and continue critical operations with minimal disruption. This will help the Regulated Entity maintain operational continuity and resilience in the face of evolving cyber threats.

For further details about Cyber resilience controls, Please Refer to Domain 9 of CBK Cyber Resilience baselines

10.Training, Testing and Continuous Improvement

Overview: This domain shall establish mechanisms for validation, awareness, and review, to enhance preparedness and embed resilience culture and drive continuous improvement. This will help the Regulated Entity improve resilience capabilities through continuous learning and testing.

10.1 Training, Testing and Exercising

Objective: To ensure the effectiveness of operational resilience plans and decision-making capabilities under disruption scenarios. Regulated Entities shall conduct regular training and testing activities to validate response procedures, assess resilience capabilities, and incorporate lessons learned into improvement initiatives.

10.1.1 Table-Top Exercises

10.1.1.1. Tabletop exercises shall be conducted at least annually to test the effectiveness of operational resilience plans and decision-making processes under simulated disruption scenarios with respective stakeholders within the regulated entity.

10.1.1.2. Scenarios shall be realistic, relevant to the regulated entity's operating context, and clearly defined with objectives. Examples may include function-specific, location-based, process-level, or High risks identified in the risk assessment.

10.1.1.3. Defined test scenarios shall cover the activation of operational resilience plans (BCP, IT DRP).

10.1.2 Business Continuity and Disaster Recovery Testing

10.1.2.1. Business continuity and Disaster recovery tests shall be conducted at least annually. Testing shall cover both business process continuity and IT systems recovery.

10.1.2.2. Tests shall be designed to validate:

a) Verify compliance with RTO and RPO targets for critical systems and data;
b) Functionality of alternate work locations; and
c) End to end recovery across the business unit and systems.

10.1.3 Crisis Simulation

10.1.3.1. Full-scale or partial crisis simulations shall be conducted at least annually to test the effectiveness of operational resilience plans and decision-making processes under simulated disruption scenarios.

10.1.3.2. Scenarios shall be developed to reflect high-impact, realistic disruption events that test the regulated entity's ability to manage complex and evolving crises. Scenarios may include multi-layered incidents such as cyberattacks, infrastructure failure, critical third-party disruption, or concurrent operational and reputational risks.

10.1.3.3. Defined test scenarios should cover the activation and involvement for crisis management team and other response teams as applicable.

10.1.4 Sector Wide Simulation

10.1.4.1. Regulated Entities shall participate in sector-wide simulation exercises coordinated by CBK where applicable. These exercises are designed to assess the readiness of the regulated entities to respond to large-scale, systemic disruptions affecting the broader banking ecosystem.

10.1.5 Continuous Improvement

10.1.5.1. Regulated Entities shall ensure that detailed results of all exercises and tests are documented for future reference and continuous improvement. The documentation shall include, at a minimum:

a) Document the objectives and scope of the exercised plan;
b) Document the participants;
c) Exercise / test results;
d) Document lessons learnt and the required improvements; and
e) In case of failure, Capture the root-cause of the failure and remediation actions should be tracked to successful conclusion.

10.1.5.2. Regulated Entities shall report the testing results to the Executive/Senior Management.

10.1.6 Training and Awareness

10.1.6.1. Regulated Entities shall ensure that all internal employees, contractors, and relevant third-party staff within the regulated entity are:

a) Familiar with relevant parts of operational resilience policies and plans
b) Familiar with their roles and responsibilities during disruptive incidents

10.1.6.2. Specialized awareness training shall be provided once on an annual basis to employees involved in resilience related disciplines to achieve the required level of experience, skills, and competences.

10.1.6.3. Specialized awareness training for the top management shall be delivered at least annually, to ensure they understand their roles in developing operational resilience culture.

10.1.6.4. Regulated Entities shall retain relevant documented information as evidence of all conducted awareness and training programs, including attendance records and assessment results.

10.1.6.5. Regulated Entities shall measure the effectiveness of the training and awareness program.

11.Exceptions Under the CORF

Any exception or exemption to one or more controls outlined in this Operational Resilience Baselines requires regulated entities to submit a formally justified exception request, including proposed compensating controls. This request must be submitted to the CBK for evaluation and approval before any exception or exemption can be granted.

12.Appendix

12.1 Incident Escalation and reporting to CBK

12.1.1 Initial Notification

High and Medium - Initial Notification			
Regulated Entity Name &	Regulated Entity Name	Date / Time of report	DD MMM YYYY HHMM
Crisis Response Lead Name	Lead Name Telephone	incident reference #	Unique identifier Regulated entity name – INC-Year- 001 > Regulated entity first incident
Severity impact rating	As per severity impact matrix in section 8.1.1		
Description of Incident	Describe the Incident		
Timeline of incidents	Enter description		
Mitigation effort	Enter description		
Estimated Financial Loss	Enter a value		
Estimated time to resolution	Enter description		
Risks to resolution	Enter description		
Support Requested from CBK	Enter description		

12.1.2 Situation Report

High and Medium - Situation Report				
Regulated Entity name	Name			
Severity impact rating	As per severity impact matrix in section 8.1.1		incident reference #	Unique identifier Regulated entity name – INC-Year-001- SITREP1 -> indicating this is the first situation report
Current Situation				
Current Situation as of	Date:	DD MMM YYYY	Time:	HHMM
Description of the Incident				
Enter description on what is known about the incident; add key facts – what has happened, where did it happen, when did it happen, who has been affected				
Cause				
1. What is your current understanding of what caused the incident?	Enter description			
2. Was the source internal, external, or unknown?	Enter description			
Impact updates				
1. Operations	Enter description			
2. Legal / Regulatory	Enter description			
3. Reputation	Enter description			
4. Theft and data breach	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 resolve 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 resources might become affected?	Enter description
Questions	
1. What other information should CBK know?	Enter description
2. Support Requested from CBK?	Enter description

12.1.3 Closure Report (High and Medium Incidents)

High and Medium - Closure Report				
Regulated Entity name	Name			
Severity impact rating	As per severity impact matrix in section 8.1.1		incident reference #	Unique identifier Regulated entity name – INC-Year-001-Close
Closure date as of	Date:	DD MMM YYYY	Time:	HHMM
1. Brief Description of the Incident	Enter description			
2. Brief Description of the impacts	Enter description			
3. Brief description of response plan and action	Enter description			
4. Parties involved in response action and their role, if applicable	Enter description			
5. Role played by CBK, if applicable	Enter description			
6. Final Financial loss	Enter a value			
7. Corrective / Preventive Measures (Next Steps)	Enter description			
8. Temporary/Permanent Preventive Measure	Enter description (Temporary or Permanent)			
9. Deadline of Temporary Preventive Measure (if temporary)	Enter description			

10. Permanent Preventive Measure after Deadline (if temporary)	Enter description
11. Lessons learned	Enter description

12.1.4 Closure Report (Monthly Low Incidents)

Low Incidents Closure Report ***Note: please provide a consolidated view of all low incidents occurred during the month***	
Regulated Entity name	Name
Date range included	DD MMM YYYY - DD MMM YYYY
1. Facility/Physical Security Incidents	
Total Number of Incident	Enter total number of low incidents occurred throughout the Month
Summary overview of the incidents	Enter description
Summary overview of response actions taken to incidents	Enter description
Summary overview of impacts	Enter description
Summary of lessons learned, and further actions needed	Enter description
2. Technology/System Outage	
Total Number of Incident	Enter total number of low incidents occurred throughout the Month
Summary overview of the incidents	Enter description

Summary overview of response actions taken to incidents	Enter description
Summary overview of impacts	Enter description
Summary of lessons learned, and further actions needed	Enter description
3. Cybersecurity-related Incidents	
Total Number of Incident	Enter total number of low incidents occurred throughout the Month
Summary overview of the incidents	Enter description
Summary overview of response actions taken to incidents	Enter description
Summary overview of impacts	Enter description
Summary of lessons learned, and further actions needed	Enter description
4. Third Parties related Incidents	
Total Number of Incident	Enter total number of low incidents occurred throughout the Month
Summary overview of the incidents	Enter description
Summary overview of response actions taken to incidents	Enter description
Summary overview of impacts	Enter description

Summary of lessons learned, and further actions needed	Enter description
5. Operation related Incidents	
Total Number of Incident	Enter total number of low incidents occurred throughout the Month
Summary overview of the incidents	Enter description
Summary overview of response actions taken to incidents	Enter description
Summary overview of impacts	Enter description
Summary of lessons learned, and further actions needed	Enter description
Others	
Enter description on what is known about the incident; add key facts – summary of incident, response action taken, impact and lessons learned	

12.2 Terms and Definitions

Term	Definitions
Business Process	A set of interrelated or interacting activities that contribute to the delivery of a core function (corporate level) or a business plan (local level). For example, "KASSIP settlement".
Crisis	Any unstable or crucial time, or rapidly occurring unplanned event, real or perceived, whose outcome can negatively impact the health or safety of employees, customers, or members of the community in which we operate, our reputation, stability, or ability to operate our business, our shareholders, or our customers.
Impact	Impact is the qualitative estimate of the potential consequences that a threat can cause to a given facility. It takes into consideration impacts to Buildings, Equipment, Technology, and Human Resources and Third-Party vendors/ suppliers.
Incident	An incident is an event that could lead to loss of, or disruption to, operations, services, activities, or functions. An incident can be managed by -standard operating processes within normal business tolerance. If it is not managed, an incident can escalate into an extraordinary event or a crisis.
Inherent Risk	The risk without considering the existing mitigating factors. Inherent Risk Rating is calculated as a function of the Impact and the Likelihood of Occurrence of a threat. It identifies how vulnerable a facility or location is to a specific threat.
Likelihood	Likelihood is the degree of certainty of an event occurring; it is an estimate based on frequency of occurrence and is gauged by historical data.
Management System	Set of interrelated or interacting elements to establish policies and objectives, and processes to achieve those objectives.
Prioritized Activities	Activities that are critical and must be given priority when recovering from a disruptive incident to reduce the impacts.

Term	Definitions
Process Owner	Process owners are responsible for the management of processes within the organization.
Recovery	Retrieval or recapturing of normal or prior state.
Residual Risk	Residual risk is the level of risk remaining after all mitigating controls have been taken to reduce the likelihood and/or impact of a specific threat.
Resiliency	The ability to anticipate, withstand, respond to, and recover from major operational and banking disruptive events. BCMS makes a significant contribution to our overall resiliency, alongside other risk mitigation activities. It includes our ability to learn from risk events when they occur and to adapt accordingly.
Resources	Resources include information, skills, people, technology, assets, and premises, which are obtained and used by the organization to achieve its goals and objective.
Tabletop Exercise	Technique for rehearsing emergency teams in which participants review and discuss the actions they would take according to their plans, but do not perform any of these actions; can be conducted with a single team, or multiple teams, typically under the guidance of exercise facilitators.
Threats	List of threats in scope for this assessment that are introduced by the events.

12.3 Appendix - Glossary

Term	Definition
CBK	Refers to the “Central Bank of Kuwait”.
CORF	Refers to the “Cyber and Operational Resilience Framework”.
ORB	Refers to the “Operation Resilience Baseline”.
Business Continuity (BC)	The ability of the regulated entity to continue its prioritized activities at predetermined levels after the occurrence of a disruptive incident.
Business Continuity (BCMS)	A business continuity management system (BCMS) is a proactive framework that ensures a regulated entity can respond effectively to disruptions, safeguarding key processes, stakeholders, and reputation. It's an integral part of overall management, focusing on establishing and improving business continuity capabilities.
Business Continuity Plan (BCP)	The documents that detail the recovery steps and actions to recover in the event of disruption.
IT Disaster Recovery Plan (IT DRP)	A documented strategy and set of procedures that outlines how a regulated entity’s IT systems, applications, and data will be restored after a disruption or disaster.
Business Impact Analysis (BIA)	It is the process for analyzing business activities and the impacts of disruptive incidents that may happen over time.
Technology Impact Analysis (TIA)	It is the process for analyzing how disruptions to IT systems, applications, and infrastructure impact business operations. It helps identify critical technologies, assess their dependencies, and evaluate the consequences of downtime.
Maximum Allowable Outage (MAO) / Maximum Acceptable Outage (MAO)	Time it would take for adverse impacts, which might arise because of not providing a product / service or performing an activity, to become unacceptable.
Maximum Tolerable Period of Disruption (MTPD)	Time that a business process can be disrupted before the regulated entity’s survival is at risk or it suffers unacceptable consequences.

Term	Definition
Recovery Point Objective (RPO)	The recovery target objective of acceptable data loss before it has an adverse effect on business operations, service, or product. Recovery Point Actual (RPA) is the confirmed actual value realized through testing or actual disruptive events.
Recovery Time Objective (RTO)	Time span after the occurrence of an incident in which an activity or product should be restarted or resources and assets should be regained.
Single Point of Failure (SPOF)	A single source of a service, activity and/or method whose unavailability would lead to the failure of a key business activity and/or dependency.
Incident Management Team (IMT)	A designated group of trained individuals responsible for managing and responding to incidents (e.g., IT outages, cyberattacks, natural disasters, or other critical events) to minimize impact and restore normal operations.
Crisis Management Team (CMT)	A group of senior leaders and specialists responsible for strategically managing and responding to a crisis that could severely impact a regulated entity's people, reputation, operations, or financial stability.
Service Level Agreement (SLAs)	A formal, documented contract between a service provider and a customer (internal or external) that defines the specific level of service expected, along with the metrics, responsibilities, and remedies if those expectations are not met.
Key Performance Index (KPIs)	Are measurable values that show how effectively an individual, team, department, or regulated entity is achieving strategic or operational goals.
Key Risk Indicators (KRIs)	Are metrics used to measure the level of risk exposure in regulated entity. They serve as early warning signals that a potential threat or risk may be emerging and help regulated entity take proactive action to avoid or mitigate it.
Risk Assessment	Risk Assessment analyses the regulated entity for vulnerabilities, examines potential threats associated with those vulnerabilities, and evaluates the resulting risks.

Term	Definition
Banking and Financial Sector and Other CBK Regulated Entities	All entities that are regulated by CBK including Local Banks, Foreign Banks, Exchange Companies, payment service providers, Open Banking Service Providers, and other regulated Finance Companies.
Kuwaiti banks	Refers to banks that have Kuwaiti promoters including Islamic, Conventional, and specialized banks.
Foreign banks	Foreign Banks in the state of Kuwait that are authorized by CBK.
Local banks	Refers to all Banks including the Kuwaiti Banks, and the Foreign Banks authorized by CBK.
Regulated Entity	Refers the following: ● Kuwaiti Banks ● Foreign Banks ● Finance Companies ● Exchange Companies ● E-Payment of Funds Companies ● Credit Information Companies ● Open Banking Service Providers
Responsibility/ Responsible person	The responsible person is the individual(s) who 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.
ISO/IEC	International Organization for Standardization/ International Electrotechnical Commission
BCI	The Business Continuity Institute

Chapter 6:
Third-Party Risk Management Baselines

DOCUMENT CONTROL

Date	Version	Author	Change Reference	Reviewer/ Approver
03 Dec 2025	1.0	Central Bank of Kuwait	First Release	Central Bank of Kuwait

TABLE OF CONTENTS

1. Introduction

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) acknowledges that Third-Party Risk Management (TPRM) is essential for maintaining banking and financial sector stability and consumer trust. As a result, CBK is introducing Third-Party Risk Management Baselines to mandate all Regulated Entities to build and sustain strong and comprehensive capabilities in managing third-party relationships.

Third-Party Risk Management Baselines (hereinafter referred to as 'Baselines') have been developed to ensure a consistent level of third-party risk controls across all Regulated Entities and to strengthen the Kuwaiti Banking and Financial sector's ability to withstand, recover and learn from disruptive events. The Baselines have been designed in line with CBK's regulations, instructions and guidelines, prevalent international operational resilience standards.

1.1 Objectives

To strengthen risk governance across the banking and financial sector, the Third-Party Risk Management (TPRM) baseline aims to establish a standardized and comprehensive approach for managing risks arising from third-party engagements. These objectives are designed to guide regulated entities in the State of Kuwait in aligning with supervisory expectations, enhancing operational resilience, and ensuring regulatory compliance.

The key objectives of the baselines are to:

- Develop and enforce policies, procedures, and controls to mitigate identified third-party risks, ensuring compliance with regulatory requirements and industry standards.
- Ensure that third-party risk management strategies are aligned with Regulated Entities' overall business objectives and regulatory expectations.
- Define clear roles, responsibilities, and oversight mechanisms to ensure accountability in managing third-party risks across all levels of the organization.
- Establish structured methodologies for identifying, assessing, and evaluating risks associated with third-party contracts, ensuring proactive risk management.
- Conduct ongoing monitoring and periodic reviews of third-party relationships to ensure continued compliance and effectiveness of risk management strategies.
- Integrate third-party risk management with business continuity planning to ensure that critical services can be maintained or quickly restored in the event of disruptions.
- Implement data protection measures to ensure the confidentiality, integrity, and availability of data shared with or processed by third-parties.

1.2 Scope

The scope of this Third-Party Risk Management (TPRM) baselines encompasses the development, implementation, and continuous enhancement of policies, procedures, and controls aimed at effectively managing risks associated with third-party relationships across the regulated entities. These measures are intended to safeguard the resilience of critical business services and operations, while

also ensuring data confidentiality, integrity, and compliance across all domains of third-party risk. They help ensure that third-parties can withstand and recover from potential disruptions.

This baseline is applicable across key operational and strategic areas of regulated entities, control functions including:

- **Business Services and Delivery Channels** – Covering outsourced or externally supported services that directly impact customer experience and service continuity.
- **Core Infrastructure Components** – Including technology platforms, data centers, and other foundational systems that support banking operations.
- **Resources and Personnel** – Encompassing third-party staff, consultants, and service providers who contribute to operational or strategic functions.
- **Internal and External Dependencies** – Addressing interlinked processes, systems, and entities that rely on or interact with third-party arrangements.

1.3 Applicability

The Baselines are applicable to all Regulated Entities supervised by the CBK and the compliance to Baselines is subject to CBK's supervision/ assessment. Furthermore, the Baselines are applicable to Regulated Entities, their employees, third-party vendors, and third-party vendor staff.

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

1.4 Target Audience

The Baselines are issued for the Board of Directors, Executive/Senior Management, Third-Party Risk Management professionals and any other personnel who are responsible for establishing, implementing, and ensuring compliance with CBK directives.

1.5 Baseline Assessment and Risk Reporting

Regulated Entities shall follow a structured approach, which assists in implementing the applicable controls as specified in the Baselines. This approach includes:

b) **Periodic / ad hoc assessment and reporting:** Regulated Entities shall conduct periodic / ad hoc 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 baseline assessment, plans, exceptions, and exclusions and may conduct necessary inspection.

2. Baselines Structure

The TPRM Baselines are structured as domains, sub-domains, control areas, and controls as defined below:

- The domain specifies the intent for a given area;
- The sub-domain establishes the objective;
- The control area groups related controls within the sub-domain, providing structured focus on specific aspects of the objective; and
- The controls specify applicable baselines that shall be covered under each sub-domain and control area.

Structure:

X. (Domain)
X.1 (Sub-Domain)
X.1.1 (Control Area)
X.1.1.1 (Control)

Example:

3. Governance Structure and Oversight
3.1 TPRM Policy and Strategy
3.1.1 TPRM Policy
3.1.1.1 Regulated entities shall develop and maintain a TPRM policy that…

2.1 Domains

The TPRM Baselines have been logically grouped into 13 domains and 46 sub-domains based on the nature of controls. The controls specified within each domain and sub-domain collectively assist in establishing consistent third-party risk management controls within Regulated Entities and achieving the objectives of the Baselines. The identified domains of the Baselines are:

a) **Governance Structure and Oversight:** This domain shall enable Regulated Entities to establish a robust framework for Third-Party Risk Management (TPRM), aligning policies and strategies with organizational goals and regulatory requirements. It fosters accountability, strategic oversight, and continuous improvement through clear roles, rigorous approvals, and periodic reviews, enhancing resilience against evolving risks.

b) **Risk Management Framework:** This domain shall ensure effective management of third-party risks by identifying critical services, assessing risks across multiple dimensions, and mapping dependencies to enhance operational resilience and inform business continuity planning.

c) **Contractual Agreements Considerations:** This domain shall define the legal and compliance obligations between the Regulated Entities and third-parties through detailed contracts. This will help Regulated Entities ensure preparedness for service restoration under various disruption scenarios.

d) **Risk Assessment and Monitoring:** This domain shall establish a robust process for the systematic identification, assessment, and continuous monitoring of risks—particularly those impacting critical IT systems and non-IT business operations.

e) **Business Continuity Management & Disaster Recovery:** This domain shall establish requirements for third-party service providers, to maintain continuity of externally delivered critical services. This will help Regulated Entities assess, monitor, and manage third-party resilience capabilities.

f) **Incident Management:** This domain shall establish requirements for third-party incident management, ensuring effective detection, response, and resolution to enhance security and resilience.

g) **Data Protection and Confidentiality:** This domain shall define third-party data management practices to maintain ensure data security and compliance, protecting sensitive data throughout its lifecycle.

h) **Sub-contracting:** This domain shall ensure third-party sub-contracting arrangements are disclosed and approved, maintaining oversight and control to adhere to vendor risk management policies and mitigate associated risks.

i) **Exit Strategy:** This domain shall establish the requirements for planned and secure disengagement from third-party relationships, ensuring continuity of critical services, protection of sensitive data, and minimal disruption during transition or termination. It includes defining exit criteria, transition support, data return or destruction protocols, and contractual safeguards to support a smooth and compliant exit process.

j) **Storage of Data:** This domain establishes the protection measures of sensitive data through secure storage practices, supporting compliance and resilience against data loss and unauthorized access.

k) **Cross-Border Transaction:** This domain shall establish compliance measures for cross-border transactions, ensuring adherence to legal, regulatory, and privacy requirements to mitigate risks and uphold financial integrity.

l) **Usage of Cloud Service Provider:** This domain shall ensure Regulated Entities effectively manage the risks associated with cloud service providers, ensuring compliance across jurisdictions, and maintaining cloud security, which is crucial for safeguarding data.

m) **Inter-Affiliates:** This domain shall establish the requirements for managing affiliate engagements in an effective way to uphold compliance, mitigate risks, and maintain services continuity.

2.2 Sub-Domains

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

Governance Structure and Oversight	Risk Management Framework	Contractual Agreements Considerations	Risk Assessment and Monitoring	Business Continuity Management & Disaster Recovery	Incident Management	Data Protection and Confidentiality	Sub-contracting	Exit Strategy	Storage of Data	Cross-Border Transaction	Usage of Cloud Service Provider	Inter-Affiliates
TPRM Policy and Strategy	Critical Third-Party Service Identification	Contractual Safeguards	Ongoing Monitoring of Critical Third Parties	Business Continuity Plans	Incident Detection and Monitoring	Data Encryption and Masking	Disclosure of Subcontractor and Approval from Regulated entities	Exit Strategy Planning	Data Storage Security	Regulatory & Legal Compliance	Cloud Security	Approval
Roles and Responsibilities	Risk Identification and Assessment Methodology	Legal Binding Agreement	Identification, Assessment, and Mitigation	Data Back up and Replication	Incident Escalation and Communication Protocols	Data Retention and Disposal	Monitoring and Oversight	Exit Clauses	Storage Lifecycle Management	Due Diligence & KYC/AML		Due Diligence and Periodic Review
Board and Senior Management Oversight	Dependency Mapping to Critical Processes	Regular Monitoring and assessment	Risk Classification	Periodic Testing of DR Capabilities	Root Cause Analysis	Data Classification and Handling Policies		Data Handling	Data Integrity and Availability	Secure Data Transfers & Privacy		Customer Consent
Approvals and Periodic Reviews		Health Safety & Environment		Recovery and Restoration Procedures						Monitoring, Reporting & Audit		Foreign Affiliates
		Financial Viability		Business Continuity								Resource Planning

Governance Structure and Oversight	Risk Management Framework	Contractual Agreements Considerations	Risk Assessment and Monitoring	Business Continuity Management & Disaster Recovery	Incident Management	Data Protection and Confidentiality	Sub-contracting	Exit Strategy	Storage of Data	Cross-Border Transaction	Usage of Cloud Service Provider	Inter-Affiliates
				Management & Recovery								
		Compliance (Geopolitics, Regulatory, Organizational, Country and Legal)										
		Corporate Governance										

Table 1: Domains and Sub-Domains of TPRM Baselines

3. Governance Structure and Oversight

Overview: This domain shall enable Regulated Entities to establish a robust framework for Third-Party Risk Management (TPRM), aligning policies and strategies with organizational goals and regulatory requirements. It fosters accountability, strategic oversight, and continuous improvement through clear roles, rigorous approvals, and periodic reviews, enhancing resilience against evolving risks.

3.1 TPRM Policy and Strategy

Objective: To ensure the establishment and maintenance of a comprehensive TPRM policy and strategy that defines clear objectives, aligns with the organizational goals, and incorporates best practices, thereby facilitating effective governance, accountability, and continual adaptation to changes in third-party risk landscape.

3.1.1 TPRM Policy

3.1.1.1. Regulated entities shall develop and maintain a TPRM policy that:

a) defines TPRM scope, activities that could be outsourced and not outsourced, Executive/Senior Management's commitment, roles and responsibilities, enforcement mechanisms, and deterrents for non-compliance;

b) incorporates relevant international best practices, frameworks, and standards;

c) aligns with business objectives, relevant organizational policies, legal, regulatory, and contractual requirements

3.1.1.2. The TPRM policy shall be defined, approved, implemented, communicated, enforced, and made accessible to all employees.

3.1.1.3. The TPRM policy shall be reviewed and updated annually or upon significant changes in the third-party ecosystem.

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

3.1.1.5. The TPRM policy shall be approved by the Executive/Senior Management and authorized by the Board to ensure alignment with the Entity's overall objectives and the proper management of third-party risks.

3.1.2 TPRM Strategy

3.1.2.1. The Regulated Entities TPRM strategy shall include:

a) define the desired TPRM maturity level and include clear objectives aligned with organizational goals and business objectives;

b) include a roadmap with timelines for achieving strategic objectives;

c) include requirements for continual review and validation of alignment of the TPRM program with strategic objectives;

d) identify the responsibility and accountability for strategy implementation and monitoring.

3.1.2.2. The TPRM strategy shall be defined, approved, and implemented, where:

a) the strategy shall undergo a formal and documented review on an annual basis;

b) the strategy shall also be subject to change-driven reviews triggered by significant internal or external factors, including:

i. Significant shifts in the third-party threat landscape (e.g., onboarding of critical vendors, outsourcing of key services, newly identified risks);

ii. New or updated regulatory, legal, or sectoral requirements;

3.2 Roles and Responsibilities

Objective: To ensure clear definition and assignment of roles and responsibilities across all functions involved in TPRM, fostering accountability, collaboration, and strategic oversight in the management of third-party risks.

3.2.1 Defined Ownership

3.2.1.1. Regulated entities shall assign explicit ownership of third-party risk to designated functions such as Risk Management, Procurement, Legal, Business, Finance, Information Security, etc. Each function should be responsible for managing risks within its domain, ensuring that third-party engagements are assessed, monitored, and governed appropriately.

3.2.2 Three Lines of Defense Model

3.2.2.1. Regulated entities shall implement a structured approach to risk governance using the Three Lines of Defense model:

1. First Line: Business units and operational teams that engage directly with third-parties are responsible for identifying, assessing, and managing risks during onboarding and throughout the lifecycle of the relationship.
2. Second Line: Risk, Compliance, and Legal functions provide oversight, develop policies and frameworks, and support the first line in implementing effective controls.
3. Third Line: Internal Audit performs independent assurance on the adequacy and effectiveness of the TPRM framework and its implementation.

3.2.3 Documentation and Communication

3.2.3.1. Regulated entities shall clearly document roles and responsibilities in TPRM policies, procedures, and charters. Ensure that all stakeholders are informed of their duties and are trained to fulfil them effectively.

3.3 Board and Senior Management Oversight

Objective: To ensure effective oversight and strategic direction by the Board and Senior Management, facilitating alignment of TPRM with organizational goals and regulatory requirements. This includes empowering dedicated functions and committees to manage third-party risks proactively and ensuring resource allocation for sustainable implementation.

3.3.1 Board of Directors

3.3.1.1. The Board of Directors (hereinafter referred as, Board) shall serve as the ultimate approving authority for the Third-Party Risk Management (TPRM) strategy. It shall also provide authorization for the TPRM policy, ensuring alignment with the entity's overall risk appetite and regulatory obligations.

3.3.1.2. The Board shall ensure the allocation of adequate financial, technological, and human resources to support the effective implementation and sustainability of the TPRM framework.

3.3.1.3. The Board shall mandate the establishment of a dedicated TPRM Oversight Committee, with clearly defined responsibilities and authority to oversee third-party risk activities.

3.3.1.4. The Board shall receive periodic reports (at least quarterly) from the TPRM Oversight Committee or relevant executive functions. These reports shall include:

- Updates on the third-party risk posture;
- Emerging threats and vulnerabilities;
- Regulatory developments and compliance status;
- Status of remediation actions and incident responses.

3.3.2 TPRM Oversight Committee

3.3.2.1. The TPRM Oversight Committee shall be chaired by a designated senior executive and shall composed of senior representatives from key functions, including:

- Head of TPRM function;
- Procurement and Vendor Management;
- Legal and Compliance;
- Information Security and Technology;
- Business Units with critical third-party dependencies;
- Business Continuity and Risk Management functions;
- Internal Audit (as an observer).

3.3.2.2. The Committee shall be chaired by a senior executive with expertise in third-party risk, governance, and regulatory compliance.

3.3.2.3. The Committee shall develop and maintain a formal charter, approved by the Board, which shall include:

- The Committee's mandate and objectives;
- Membership composition and roles;
- Meeting frequency (minimum quarterly) and quorum requirements;
- Reporting lines and escalation protocols.

3.3.2.4. The Committee shall be responsible for:

- Reviewing and endorsing the TPRM strategy and policy;

- Monitoring program effectiveness through Key Risk Indicators (KRIs), Key Performance Indicators (KPIs), and resource utilization;
- Reviewing risk assessments and classifications of critical third-party service providers;
- Overseeing incident response, post-incident reviews, and closure of remediation actions related to third-party failures;
- Ensuring the implementation of training and awareness programs across the organization;
- Staying aware of regulatory changes, industry developments, and ensuring ongoing compliance with applicable laws and standards.

3.3.3 Executive and Senior Management

3.3.3.1. Executive and Senior Management shall ensure the effective execution of the TPRM framework, including integration with enterprise risk management, business continuity, and operational resilience programs.

3.3.3.2. Senior Management shall allocate sufficient resources—financial, technological, and personnel to support the TPRM lifecycle, including onboarding, monitoring, and offboarding of third-party relationships.

3.3.3.3. They shall foster a culture of risk awareness, ethical conduct, and continuous improvement in third-party engagements across all levels of the organization.

3.3.3.4. Executive Management is responsible for reviewing and implementing actions arising from assessments and audits. These evaluations shall be used to inform strategic decisions and drive enhancements in the program.

3.3.4 Third-Party Risk Management Function

3.3.4.1. The head of the Third-Party Risk Management function shall be responsible for defining and reviewing the TPRM strategy

3.3.4.2. Regulated entities shall establish a Third-Party Risk Management (TPRM) function with clearly defined roles and responsibilities, empowered by executive/senior management and overseen by the BRC Committee or equivalent authority.

3.3.4.3. The TPRM function shall be appropriately staffed with personnel possessing knowledge in vendor risk, compliance, legal, and information security, commensurate with the scale and complexity of third-party engagements.

3.3.4.4. The TPRM function shall be responsible and accountable for establishing and maintaining policies, procedures, and tools to identify, assess, mitigate, and monitor risks associated with third-party relationships.

3.3.4.5. The function shall coordinate with business units, procurement, legal, compliance, finance (or equivalent), IT and Information Security to ensure a holistic approach to third-party risk management across the organization.

3.3.4.6. The Head of TPRM shall ensure that third-party risk assessments, due diligence, and ongoing monitoring activities are conducted consistently and that risk findings are escalated and addressed in a timely manner.

3.3.4.7. Periodic reporting on third-party risk posture, emerging risks, and remediation status shall be provided to the TPRM Oversight Committee, at least quarterly or as required by significant changes in the third-party landscape.

3.3.4.8. Periodic reporting on third-party risk posture, emerging risks, and remediation status shall be provided to the TPRM Oversight Committee, at least quarterly or as required by significant changes in the third-party landscape.

3.4 Approvals and Periodic Reviews

Objective: To ensure rigorous and systematic approvals and periodic reviews of the TPRM policy, strategy, and risk assessments, maintaining alignment with regulatory requirements and industry standards.

3.4.1 Annual Review and Approval

3.4.1.1. The TPRM policy and overarching strategy shall be reviewed and formally approved by senior management or the designated governance committee at least annually. Additional reviews shall be conducted upon the occurrence of significant changes in the regulatory landscape, business operations, or risk environment.

3.4.2 Periodic Risk Assessment Reviews

3.4.2.1. Third-party risk assessments, including due diligence outcomes, control effectiveness, and residual risk ratings, shall be reviewed periodically based on the criticality and risk profile of the third-party. High-risk third-parties shall be reviewed annually, medium-risk every two years, and low-risk every three years.

3.4.2.2. Controls implemented to mitigate third-party risks shall be evaluated regularly to ensure they remain effective and aligned with current threats, vulnerabilities, and compliance requirements.

3.4.2.3. All approvals, reviews, and updates to the TPRM policy, strategy, and risk assessments shall be documented. The review process shall ensure continued alignment with applicable regulatory guidelines and leading industry standards.

4. Risk Management Framework

Overview: This domain shall ensure effective management of third-party risks by identifying critical services, assessing risks across multiple dimensions, and mapping dependencies to enhance operational resilience and inform business continuity planning.

4.1 Critical Third-Party Service Identification

Objective: To ensure the identification and classification of third-party services by evaluating their impact on essential business functions, data sensitivity, regulatory dependencies, and maintain a centralized inventory for effective risk management and continuity planning.

4.1.1 Impact on Critical Business Services

4.1.1.1. Regulated entities shall evaluate the extent to which a third-party supports essential business functions or services that, if disrupted, could significantly affect operations or customer outcomes.

4.1.2 Data Sensitivity and Volume

4.1.2.1. Regulated entities shall assess the nature and volume of data shared with or processed by third-parties, based on its classification.

4.1.3 Regulatory and Operational Dependencies

4.1.3.1. Regulated entities shall consider dependencies arising from regulatory obligations, licensing requirements, or operational interlinkages that may elevate the criticality of the third-party.

4.1.4 Centralized and continuously updated inventory

4.1.4.1. Regulated Entities shall maintain a centralized and periodically updated inventory of all third-party relationships, clearly flagging those classified as critical. This inventory should be integrated with risk registers and business continuity plans.

4.1.4.2. The centralized inventory shall be maintained by the designated TPRM function and updated at least quarterly or upon any significant change in third-party relationships.

4.2 Risk Identification and Assessment Methodology

Objective: To ensure the identification and evaluation of third-party risks across multiple dimensions, enabling prioritized oversight and effective treatment through risk scoring, due diligence, and ongoing monitoring.

4.2.1 Multi-Dimensional Risk Assessment

4.2.1.1. Regulated entities shall evaluate third-party risks across key dimensions, including:

a) financial risk
b) operational risk
c) cybersecurity and information security risk
d) legal and contractual risk
e) reputational risk
f) regulatory and compliance risk

4.2.2 Risk Scoring and Prioritization

4.2.2.1. Regulated entities shall apply quantitative and qualitative risk scoring to classify third-party relationships into tiers based on service criticality, data sensitivity, and customer impact, enabling prioritized oversight and mitigation.

4.2.3 Due Diligence and Ongoing Monitoring

4.2.3.1. Regulated entities shall conduct thorough due diligence during onboarding and implement periodic reassessments based on risk tiering and performance indicators.

4.3 Dependency Mapping to Critical Processes

Objective: To ensure the identification and documentation of single points of failure and interdependencies, and concentration risks integrating these insights into business continuity planning to mitigate cascading risks and enhance operational resilience.

4.3.1 Identify Single Points of Failure and Concentration Risks

4.3.1.1. Regulated entities shall highlight areas where reliance on a single third-party or service could lead to operational disruption.

4.3.1.2. Regulated entities shall identify third-party concentration risk exposure where dependency on a single vendor is on multiple critical services.

4.3.2 Interdependencies and BCP Integrations

4.3.2.1. Regulated entities shall document interconnections between third-parties and their internal processes, systems, or downstream dependencies to other vendors to assess cascading risk impacts.

4.3.2.2. Regulated entities shall ensure that dependency mapping informs BCP and disaster recovery strategies, enabling timely response and recovery in the event of third-party failure.

5. Contractual Agreements Considerations

Overview: This domain outlines the foundational legal, regulatory, and governance expectations that shall be embedded within third-party contractual arrangements. It ensures that Regulated Entities maintain enforceable agreements that support operational resilience, regulatory compliance, and risk mitigation across all third-party engagements. These provisions are critical to ensuring service continuity, accountability, and oversight during normal operations and disruption scenarios.

5.1 Contractual Safeguards

Objective: To ensure that all contracts with third-parties contain clear, enforceable provisions that address the regulated entities' risk management, resilience, and regulatory requirements. This includes specifying obligations for data protection, business continuity, incident reporting, regulatory compliance, and service levels; identifying critical services and single points of failure; and establishing rights for audit, monitoring, and termination. These safeguards enable the Regulated Entities to effectively manage third-party risks, maintain operational resilience, and ensure compliance with applicable laws and regulations.

5.1.1 Scope of Service, Termination Clauses, Right to Audit

5.1.1.1. Regulated entities shall ensure that Third-Party obtain, maintain, and provide evidence of all necessary approvals, licenses, permits, and authorizations required by applicable laws and regulations to perform the contracted services.

5.2 Legal Binding Agreement

Objective: To ensure that all third-party engagements are governed by legally enforceable agreements, executed by authorized signatories, and reviewed by legal counsel. These agreements shall clearly define service scope, roles, responsibilities, and include provisions for confidentiality, liability, dispute resolution, and termination, thereby safeguarding the interests of Regulated Entities.

5.2.1 Contract Repository

5.2.1.1. Regulated entities shall maintain a consolidated repository of all third-party contracts and arrangements, including purchase orders (PO), non-PO engagements, and one-time vendor agreements, where third-parties access, process, or store Regulated entities' data. This repository shall be regularly updated, centrally accessible to authorized personnel, and structured to support oversight, compliance, and audit requirements.

5.2.1.2. Regulated entities shall ensure that all third-party engagements are governed by legally binding agreements, duly executed by authorized signatories. These agreements shall be enforceable under applicable laws and reviewed by legal counsel prior to execution. Copies of executed contracts shall be securely maintained and made available for audit or regulatory review upon request. Contracts shall clearly define the scope of services, roles and responsibilities, and incorporate comprehensive safeguarding clauses, including but not limited to:

a) right to audit the third-party and its subcontractors;
b) exit strategies, including termination rights for non-compliance and mandatory handover of assets, data, and documentation;
c) confidentiality, data privacy, and data portability/erasure obligations;

d) adherence to the entity's information and cybersecurity policies;
e) access to all records and information relevant to the outsourced activity;
f) liability for security breaches and data leakage, supported by cyber insurance or equivalent coverage;
g) escrow arrangements for source code, if applicable;
h) right to deny access to unauthorized personnel;
i) defined performance metrics (e.g., SLA, TAT, service quality) and remedies for SLA breaches;
j) visibility and control over subcontractor involvement; and
k) dispute resolution mechanisms and termination conditions.

5.2.2 Contract Execution and Enforceability

5.2.2.1. Regulated entities shall ensure that all contractual arrangements with third-parties are governed by legally binding agreements that are duly executed by authorized signatories of both parties. These agreements shall clearly define the scope of services, roles and responsibilities, confidentiality obligations, liability clauses, dispute resolution mechanisms, and termination conditions.

5.2.2.2. Regulated entities shall verify that such agreements are enforceable under applicable laws and are reviewed by legal counsel prior to execution. Copies of executed contracts shall be securely maintained and made available for audit or regulatory review upon request.

5.3 Regular Monitoring and Assessment

Objective: To establish a structured mechanism for ongoing oversight of third-party compliance with contractual obligations. This includes monitoring service delivery against defined performance metrics, verifying adherence to legal and operational clauses, and ensuring the effectiveness of subcontractor arrangements. Deviations shall be addressed through corrective actions and enhanced oversight.

5.3.1 Ongoing Oversight of Contractual Compliance

5.3.1.1. Regulated entities shall establish and implement a structured process for the regular monitoring and assessment of third-party compliance with contractual obligations. This includes:

a. evaluating service delivery against agreed performance metrics
b. verifying adherence to legal and operational clauses (e.g., scope of services, termination rights, audit provisions)
c. ensuring the effectiveness of back-to-back arrangements with subcontractors

5.3.1.2. Monitoring activities shall be documented, and any deviations or risks identified shall be escalated and addressed through corrective actions, contract amendments, or enhanced oversight measures.

5.4 Health Safety & Environment

Objective: To ensure that third-party contracts incorporate comprehensive Environmental, Health, and Safety (EHS) obligations aligned with applicable regulatory standards. This includes documented safety programs, contingency plans, valid permits, and periodic assessments to verify compliance, thereby protecting personnel, assets, and the environment.

5.4.1 Contractual adequacy

5.4.1.1. Regulated entities shall ensure that all contractual agreements with third-parties explicitly incorporate comprehensive Environmental, Health, and Safety (EHS) obligations. These contractual provisions shall:

d. align with applicable regulatory standards and cover workplace safety, environmental protection, and emergency preparedness.

e. require third-parties to maintain a formally documented EHS policy, approved by senior management, communicated to stakeholders, and periodically reviewed for relevance and effectiveness.

f. mandate the implementation of a safety program addressing high-risk operational areas such as confined spaces, hazardous energy control (Lock Out/Tag Out), hot work, working at heights, and contractor EHS management.

g. include requirements for documented contingency plans to manage pollutant releases (e.g., spills, emissions to air, water, or waste), with procedures for immediate response, mitigation, and regulatory reporting.

h. ensure third-parties maintain valid permits, have no unresolved regulatory violations in the current financial year, and conduct documented safety training for their workforce.

i. allow for periodic assessments by Regulated Entities to verify ongoing compliance with these EHS obligations.

5.5 Financial Viability

Objective: To ensure that third-parties demonstrate and maintain financial health throughout the engagement, Regulated Entities shall adopt a risk-based approach to financial viability assessments, conducting detailed reviews for critical vendors and basic checks for non-critical vendors to mitigate risks arising from financial instability.

5.5.1 Assessment of Financial Indicators

5.5.1.1. Regulated Entities shall establish a risk-based approach to assess the financial viability of third-parties throughout the engagement lifecycle. This includes incorporating contractual provisions that mandate the demonstration and maintenance of financial health:

a. the depth and frequency of financial assessments shall be proportionate to the criticality of the third-party.

b. for critical vendors, Regulated Entities shall perform comprehensive financial assessments, including analysis of key financial indicators such as credit ratings, current ratios, debt-equity ratios, profitability trends, and revenue growth.

c. for non-critical vendors, basic financial health checks — such as verification of valid trade licenses, solvency confirmation, and absence of bankruptcy proceedings — may be deemed sufficient.

d. this control supports ongoing monitoring and enables timely identification of financial instability risks that may impact service delivery or regulatory compliance.

5.6 Compliance (Geopolitics, Regulatory, Organizational, Country and Legal)

Objective: To ensure that third-parties operate in full compliance with applicable geopolitical, regulatory, organizational, country-specific, and legal requirements. This includes maintaining ABAC policies, tracking relevant legislation, disclosing litigation risks, and implementing structured compliance frameworks to support transparency and accountability.

5.6.1 Anti-Bribery and Anti-Corruption Policy

5.6.1.1. Regulated entities shall have documented and approved anti-bribery and anti-corruption policy that shall commensurate with the size, risk, and criticality of the third-party relationship, ensure that third-parties maintain a formally documented and approved Anti-Bribery and Anti-Corruption (ABAC) Policy.

5.6.1.2. The (ABAC) Policy shall be communicated to all relevant employees, contractors, and agents, and, where appropriate, incorporated into the third-party's Code of Conduct.

5.6.1.3. The (ABAC) Policy shall be reviewed and updated at regular intervals—at least annually or upon significant regulatory or operational changes. Where feasible and proportionate to the risk, regulated entities shall maintain records of bribery or corruption-related investigations or legal actions.

5.6.2 Identification of Applicable Legislation & Contractual Requirements

5.6.2.1. Regulated Entities shall ensure that third-parties identify, document, and track all relevant legislative, statutory, regulatory, and contractual security requirements applicable to their operations. Compliance shall be maintained through a structured governance framework that includes:

a. maintenance of a compliance register or tracker;

b. regular reviews and updates based on changes in laws or contracts;

c. assignment of ownership for each requirement;

d. periodic audits and assessments to verify adherence; and

e. documentation of evidence supporting compliance.

5.6.3 Litigation and Legal Exposure

5.6.3.1. Regulated entities shall ensure that third-parties disclose any litigation involving allegations of intellectual property infringement, misappropriation, or related claims. This includes cases involving the third-party itself, its directors, officers, owners, or majority shareholders, as well as any third-party products or services offered. Such disclosures shall be documented and incorporated into the entity's legal compliance and third-party risk assessment framework.

5.7 Corporate Governance

Objective: To ensure that third-parties uphold sound corporate governance practices, including disclosure of investigations or audits by regulatory bodies. This promotes ethical conduct, transparency, and accountability, and enables Regulated Entities to factor governance risks into their third-party risk assessments and oversight mechanisms.

5.7.1 Investigation

5.7.1.1. Regulated entities shall ensure that third-parties disclose any investigations or audits conducted by regulators or government agencies for alleged non-compliance with applicable laws. This includes, but is not limited to, violations related to bribery, kickbacks, or other improper payments to government officials. Disclosures shall cover the third-party itself, as well as its directors, officers, majority shareholders, affiliated entities, and employees. Such information shall be documented and factored into Regulated entities' third-party risk assessment and compliance oversight processes.

6. Risk Assessment and Monitoring

Overview: This domain shall define establishing a robust process for the systematic identification, assessment, and continuous monitoring of risks—particularly those impacting critical IT systems and business operations.

6.1 Identification, Assessment, and Mitigation

Objective: To enable Regulated Entities to systematically identify, evaluate, and address risks associated with third-party engagements. This includes conducting periodic reassessments, monitoring for emerging threats, and implementing targeted mitigation plans with defined ownership, timelines, and reporting protocols to reduce risk exposure and ensure continuity.

6.1.1 Conduct Periodic Reassessments

6.1.1.1. Regulated entities shall reassess third-party risks at defined intervals based on their risk tier, service criticality, and performance history. Trigger reassessments upon significant changes in services, regulations, threat landscape or upon renewal and breaches.

6.1.2 Identify Emerging Risks

6.1.2.1. Regulated entities shall continuously monitor for new risk vectors, including changes in legal frameworks, threat landscapes, and operational dependencies.

6.1.3 Mitigation Planning

6.1.3.1. Regulated entities shall develop and implement targeted treatment plans for identified risks. Each plan shall include:

a. defined risk owner(s)
b. specific mitigation actions
c. timelines and milestones
d. monitoring and reporting mechanisms

6.2 Risk Classification

Objective: To support differentiated oversight and resource allocation based on the risk profile of third-party engagements. Regulated Entities shall classify third-parties using inherent and residual risk criteria, and align monitoring intensity, audit frequency, and governance practices with regulatory expectations and international standards.

6.2.1 Classify Based on Inherent and Residual Risk

6.2.1.1. Regulated entities shall evaluate third-parties based on the nature of the service (inherent risk) and the effectiveness of controls in place (residual risk).

6.2.2 Determine Oversight Intensity

6.2.2.1. Regulated entities shall use classification outcomes to define the frequency and depth of due diligence, monitoring, and audit activities. High-risk third-parties should be subject to enhanced scrutiny and more frequent reviews.

6.2.3 Align with Regulatory Expectations

6.2.3.1. Regulated entities shall ensure that classification methodologies and oversight practices are consistent with regulatory guidance and leading international standards.

6.3 Ongoing Monitoring of Critical Third Parties

Objective: To ensure continuous oversight of critical third-party relationships by monitoring service performance, compliance, and emerging risks. Regulated Entities shall implement structured mechanisms including SLA tracking, risk surveillance, and automated intelligence tools to proactively identify deviations and maintain operational resilience.

6.3.1 Performance and SLA Monitoring

6.3.1.1. Regulated entities shall regularly track service delivery against agreed Service Level Agreements (SLAs) and Key Performance Indicators (KPIs) to ensure operational reliability.

6.3.2 Compliance and Risk Surveillance

6.3.2.1. Regulated entities shall monitor compliance with contractual obligations, regulatory requirements, and internal policies. Identify emerging risks such as geopolitical shifts, cyber threats, or financial instability.

6.3.3 Automated Risk Intelligence Tools

6.3.3.1. Regulated entities may leverage technology platforms that provide real-time alerts, external risk signals, and automated updates on third-party risk profiles. These tools could integrate with internal systems to support proactive decision-making.

7. Business Continuity Management & Disaster Recovery

Overview: This domain shall establish requirements for third-party service providers, to maintain continuity of externally delivered critical services. This will help Regulated Entities assess, monitor, and manage third-party resilience capabilities.

7.1 Business Continuity Plans

Objective: To ensure the adequacy of third-parties' business continuity and disaster recovery plans, formally approved and effectively implemented.

7.1.1 Business Continuity and Disaster Recovery Plans

7.1.1.1. Regulated Entities shall ensure that third-parties maintain a comprehensive Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP) that are formally documented, approved by relevant authorities, and effectively implemented.

7.2 Data Back up and Replication

Objective: To ensure third-parties maintain effective backup policies and procedures, regularly reviewing and updating them to accommodate changes in operations, technology, and regulations, while ensuring consistent replication across primary and contingency environments.

7.2.1 Policy Review and Maintenance

7.2.1.1. Regulated Entities shall ensure that third-parties periodically review and update their backup policies, procedures, and plan documents to maintain suitability, adequacy, and effectiveness. Reviews should account for changes in business operations, technology, and regulatory requirements, and shall include validation of backup and restoration processes. All updates shall be documented and approved through appropriate governance mechanisms.

7.2.2 Information Backup

7.2.2.1. Regulated Entities shall ensure that their third-parties have an approved backup policy and procedure governing the management, execution, and oversight of data backup activities. Additionally, third-party shall maintain a formally documented and authorized Backup Plan that includes:

a. information to be backed up, including data types and criticality;
b. identification of systems hosting the information (e.g., server or application names);
c. supporting IT infrastructure details (e.g., hardware specifications, storage configurations);
d. defined backup periodicity (e.g., daily, weekly, monthly, annual) based on business and data sensitivity requirements; and
e. data retention schedules aligned with applicable legal, contractual, and regulatory obligations.

7.2.3 Contingency Environments - Change Management

7.2.3.1. Regulated Entities shall ensure that third-party service providers have a formal change management process in place to ensure that all changes are consistently replicated across primary and contingency environments.

7.3 Periodic Testing of DR Capabilities

Objective: To ensure third-party service providers maintain key infrastructure in high availability mode and conduct regular resilience testing, including business continuity and disaster recovery plans, to validate and align recovery objectives with business requirements.

7.3.1 Availability of Key Infrastructure

7.3.1.1. Regulated Entities shall ensure that their third-party service providers maintain a Disaster Recovery (DR) center to support continuity of operations during major disruptions. The DR center should be geographically separated from the primary data center, preferably located in a different seismic zone, to mitigate regional risks and enhance redundancy.

7.3.1.2. Ensure all key infrastructure should be deployed in High Availability (HA) mode to ensure uninterrupted service delivery.

7.3.2 Resilience testing

7.3.2.1. Regulated Entities shall ensure that third-parties conduct periodic testing of their Business Continuity Plans (BCPs) to validate effectiveness and readiness in responding to disruptive events.

7.3.2.2. Regulated Entities shall ensure that third-parties have defined and documented Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) for all critical services provided.

7.3.2.3. Regulated Entities shall ensure that parameters be reviewed periodically and aligned with business impact assessments and agreed service-level expectations.

7.4 Recovery and Restoration Procedures

Objective: To ensure third-parties conduct regular restoration testing of backup data, verifying integrity and recoverability, and promptly addressing any discrepancies to maintain system reliability.

7.4.1 Restoration testing

7.4.1.1. Regulated Entities shall ensure that third-parties perform periodic restoration testing of backup data to verify its integrity, accuracy, and recoverability. Each test shall be documented in a Backup Restoration Log, detailing the date, scope, results, and any issues encountered.

7.4.1.2. Discrepancies or errors identified during testing shall be promptly reported to relevant stakeholders and addressed through corrective actions to ensure the reliability of backup systems.

7.5 Business Continuity Management & Recovery

Objective: To ensure the provision of contractual guarantees by third-parties through Service Level Agreements (SLAs) and defining measurable performance metrics.

7.5.1 Contractual guarantees

7.5.1.1. Regulated Entities shall ensure that third-parties offer contractual guarantees, such as Service Level Agreements (SLAs), to ensure reliability and accountability in the delivery of products and services. SLAs should define measurable performance metrics, including uptime commitments, response and resolution times, and applicable penalties or remedies for service disruptions. Regulated Entities shall ensure that documentation of all active SLAs is maintained and clearly communicated to relevant stakeholders.

8. Incident Management

Overview: This domain shall establish requirements for third-party incident management, ensuring effective detection, response, and resolution to enhance security and resilience.

8.1 Incident Detection and Monitoring

Objective: To ensure third-party service providers implement comprehensive threat detection and monitoring capabilities to enhance incident response and safeguard assets against unauthorized activities and emerging threats.

8.1.1 Threat Detection Capability

8.1.1.1. All applicable controls related to incident detection and monitoring, defined in the Cyber Resilience Baselines, shall be evaluated as a part of the assessment process.

8.1.1.2. Regulated Entities shall ensure that third-parties implement real-time security monitoring tools that continuously track and alert on unauthorized or anomalous activity within infrastructure, endpoints, and cloud systems.

8.1.1.3. Regulated Entities shall ensure that third-parties configure systems to detect abnormal behavior patterns that may indicate compromised accounts or malicious insider activity through User and Entity Behavior Analytics (UEBA).

8.1.1.4. Regulated Entities shall ensure that third-parties subscribe to and integrate actionable threat intelligence feeds to enhance detection capabilities against known indicators of compromise (IOCs) and emerging global threats.

8.1.2 Logging and Monitoring

8.1.2.1. Regulated Entities shall ensure that third-parties establish centralized and tamper-resistant logging of critical system events, with defined retention, log review schedules, and correlation to support incident detection and analysis.

8.1.2.2. Regulated entities shall ensure that third-parties enforce heightened monitoring and alerting controls around mission-critical systems, such as finance, authentication, and customer data stores.

8.1.2.3. Regulated entities shall ensure that third-parties establish processes to triage and prioritize alerts based on severity, impact, asset criticality, and data sensitivity to reduce alert fatigue and ensure rapid incident response.

8.1.2.4. Regulated entities shall ensure that third-parties define the scope of systems to be logged for incident detection purposes and conduct periodic reviews to ensure completeness and compliance with retention policies.

8.1.2.5. Regulated entities shall ensure that third-parties implement tools and protocols to detect unauthorized actions or unusual behaviors by internal users, with contextual awareness of access levels, job roles, and data movement.

8.1.2.6. Regulated entities shall ensure that third-parties configure cloud platforms (e.g., AWS CloudTrail, Azure Monitor) to capture administrative actions, user activity, and API events, ensuring alerting and retention settings are compliant.

8.1.2.7. Regulated Entities shall ensure that third-parties integrate SaaS platforms with SIEM or CASB tools and enable event-based notifications for critical activities like account takeovers and data sharing,

8.1.2.8. Regulated Entities shall offer secure, anonymous channels for employees or third-parties to report suspected cybersecurity or privacy incidents, with clear procedures for investigation.

8.2 Incident Escalation and Communication Protocols

Objective: To ensure third-party service providers establish robust communication protocols that facilitates timely and coordinated responses to mitigate risks and protect organizational reputation.

8.2.1 Internal and External Notification Criteria

8.2.1.1. Regulated entities and their third-parties shall define and maintain an incident escalation matrix outlining severity levels, responsible personnel, communication timelines, and response thresholds for various incident types.

8.2.1.2. Regulated entities shall ensure that third-parties document internal notification protocols for promptly informing senior leadership, legal, and compliance stakeholders during major or high-risk incidents.

8.2.1.3. Regulated entities shall identify legal and regulatory thresholds for incident reporting (in line with the timelines defined in the Operational Risk Baselines) and establish workflows to ensure timely notifications, from third-parties.

8.2.1.4. Regulated entities shall establish criteria, channels, and content templates for notifying affected customers of security breaches, including support channels and mitigation advice with third-parties.

8.2.1.5. Regulated entities shall define procedures for handling media inquiries, public disclosures, and social media messaging during active third-party incidents to avoid reputational damage and misinformation.

8.2.1.6. Regulated entities shall establish agreements with third-party vendors and cloud providers for mutual notification, impact assessment, and collaborative response to incidents involving shared systems or data.

8.2.2 Secure Communication Channels

8.2.2.1. Regulated entities shall ensure that third-parties have availability of secure, redundant communication tools (e.g., Signal, PGP-encrypted email) for use during incident response to prevent eavesdropping.

8.2.2.2. Regulated entities shall ensure that third-parties periodically test communication trees, escalation paths, and approval chains for incident response to verify response readiness and reduce decision-making delays.

8.2.2.3. Regulated entities shall ensure that third-parties maintain detailed logs of all internal and external communications conducted during incidents, including timestamps, recipients, and delivery confirmation.

8.3 Root Cause Analysis

Objective: To ensure the identification and resolution of root causes by third-parties for major incidents, enhancing security measures and preventing future occurrences.

8.3.1 RCA Standard and Documentation

8.3.1.1. Regulated entities shall ensure that third-parties perform and document formal Root Cause Analysis (RCA) requiring RCA for High and Medium incidents (as defined in the Operational Resilience Baselines).

8.3.1.2. Regulated entities shall ensure that third-parties compile RCA reports with background, root causes, corrective actions, and preventive recommendations, and share them with senior leadership for review and approval.

8.3.1.3. Regulated entities shall ensure that third-parties assign defined roles to security, IT, legal, and business stakeholders in the RCA process, ensuring cross-functional participation and agreement on findings.

8.3.2 Evidence Collection and Retention

8.3.2.1. Regulated entities shall ensure that third-parties collect relevant forensic evidence (e.g., logs, system images) during incident response, preserve it with documented chain-of-custody for RCA and legal purposes and enable Regulated Entities with access.

8.3.2.2. Regulated entities shall ensure that third-parties reconstruct incident timelines from detection to recovery using logs, alerts, and communications to identify gaps in detection and delays in response.

8.3.2.3. Regulated entities shall ensure that third-parties document specific control failures or process weaknesses that led to the incident and assess their effectiveness during detection, escalation, or containment.

8.3.3 Incident Documentation

8.3.3.1. Regulated entities shall ensure that third-parties review past incidents to identify trends, recurring vulnerabilities, or systemic issues contributing to repeated breaches or disruptions.

8.3.3.2. Regulated entities shall ensure that third-parties maintain a central repository of lessons learned from all security incidents and use these insights to drive future process and control improvements.

8.3.3.3. Regulated entities shall ensure that third-parties incorporate any changes identified during RCA into updated playbooks, SOPs, detection rules, or technical configurations within agreed timelines.

8.3.3.4. Regulated entities shall ensure that third-parties define KPIs for the closure of RCA action items, track them through dashboards, and periodically report progress to stakeholders.

9. Data Protection and Confidentiality

Overview: This domain shall define third-party data management practices to maintain ensure data security and compliance, protecting sensitive data throughout its lifecycle.

9.1 Data Encryption and Masking

Objective: To ensure third-parties implement robust encryption policies and procedures, safeguarding data and communications to prevent unauthorized access and ensure data confidentiality and integrity.

9.1.1 Encryption and Key Management

9.1.1.1. Regulated entities shall ensure that third-parties establish a comprehensive encryption policy that mandates the protection of sensitive data using encryption both in transit and at rest. The sensitive data can include personal data, as well as internal confidential organizational data. This policy shall specify algorithm standards, key management practices, and the scope of assets covered.

9.1.1.2. Regulated entities shall ensure that third-parties implement a centralized key management system to ensure the secure generation, rotation, storage, revocation, and disposal of cryptographic keys used in personal data encryption.

9.1.1.3. Regulated entities shall ensure that all personal data transmitted over public or untrusted networks by third-parties is encrypted using strong cryptographic protocols (e.g., TLS 1.2 or above) to prevent interception or tampering.

9.1.1.4. Regulated entities shall ensure that all personal data stored in databases, files, portable devices, or media by third-parties is encrypted using approved algorithms (e.g., AES-256), and the encryption is enforced through technical controls.

9.1.1.5. Regulated entities shall ensure that third-parties enforce encryption policies on all end-user devices (laptops, mobile phones, tablets) where personal data is stored or accessed, including mobile device management (MDM) for enforcement.

9.1.1.6. Regulated entities shall ensure that sensitive data is either masked or anonymized by third-parties before being used in development, test, or sandbox environments to prevent unauthorized access or misuse. The sensitive data can include personal data, as well as internal confidential organizational data.

9.1.1.7. Regulated entities shall ensure that third-parties assess and implement tokenization or pseudonymization techniques to reduce the identifiability of personal data, especially in analytics or multi-tenant environments.

9.1.1.8. Regulated entities shall ensure that third-parties deploy approved data masking tools to enforce consistent redaction or substitution of sensitive fields in structured and unstructured data sources.

9.1.1.9. Regulated entities shall ensure that all backup media or snapshots containing personal data in third-party ecosystem are encrypted at rest using standard encryption algorithms and stored securely with access controls.

9.1.1.10. Regulated entities shall ensure that third-parties define and apply standardized cryptographic algorithms approved by recognized bodies (e.g., AES-256, RSA 2048) and prohibit weak or outdated algorithms.

9.1.1.11. Regulated entities shall ensure that access to encrypted personal data is granted only to authorized personnel based on business need, with decryption activity monitored and logged, within third-party ecosystem.

9.1.1.12. Regulated entities shall ensure that third-parties regularly review encryption implementation across systems to ensure compliance with policy and detect any deviations or unprotected assets.

9.2 Data Retention and Disposal

Objective: To ensure third-parties establish and implement proper data retention and disposal practices, aligning with legal and regulatory requirements, and business purposes.

9.2.1 Data Retention and Archival

9.2.1.1. Regulated entities shall ensure that third-parties establish and implement a personal data retention policy that defines maximum retention periods for each data category, aligned with business purpose and legal requirements.

9.2.1.2. Regulated entities shall ensure that third-parties define and map retention periods for each processing activity, ensuring alignment with the original data collection purpose and business relevance.

9.2.1.3. Regulated entities shall ensure that third-parties identify applicable legal and regulatory requirements for personal data retention and integrate them into the organizational retention policy.

9.2.1.4. Regulated entities shall ensure that third-parties review retained personal data at regular intervals to identify records exceeding defined limits and flag them for secure deletion or archival.

9.2.1.5. Regulated entities shall ensure that third-parties implement technical and procedural safeguards to ensure personal data is permanently destroyed when it reaches end of life, using methods such as shredding, secure wiping, or degaussing.

9.2.1.6. Regulated entities shall ensure that third-parties shall log personal data disposal activities including timestamp, responsible personnel, method of destruction, and confirmation of successful deletion.

9.2.1.7. Regulated entities shall ensure that third-parties configure automated systems and applications to delete or anonymize personal data based on pre-set retention triggers and schedules.

9.2.1.8. Regulated entities shall ensure that third-parties perform periodic reviews of archived personal data to ensure ongoing necessity, legal compliance, and timely removal of redundant data sets.

9.2.1.9. Regulated entities shall ensure that third-parties contracts include enforceable clauses for secure data disposal or return upon contract termination.

9.2.1.10. Regulated entities shall ensure that third-parties document exceptions to data retention schedules, supported by legal or operational justifications, and subject to approval by the DPO or designated authority.

9.2.1.11. Regulated entities shall validate that cloud providers support complete, auditable, and timely deletion of personal data from all storage layers when requested.

9.2.2 Awareness and Training

9.2.2.1. Regulated entities shall ensure that third-parties incorporate data retention and secure disposal practices into employee privacy training programs and monitor comprehension through assessments.

9.3 Data Classification and Handling Policies

Objective: To ensure the comprehensive management and classification of data by third-parties, safeguarding data security and compliance throughout its lifecycle.

9.3.1 Data Classification and Inventory

9.3.1.1. Regulated entities shall ensure that third-parties maintain a real-time, centralized inventory of all sensitive data assets, including source, classification level, storage location, format, and assigned data owner. The sensitive data can include personal data, as well as internal confidential organizational data.

9.3.1.2. Regulated entities shall ensure that third-parties implement and enforce a classification policy to categorize personal data based on sensitivity and processing risk, assigning clear handling rules per classification.

9.3.1.3. Regulated entities shall ensure that all personal data is properly labelled or tagged within third-party storage systems and applications to indicate its classification and handling requirements.

9.3.1.4. Regulated entities shall ensure that third-parties designate responsible data owners for each personal data category to manage lifecycle, access, quality, and classification maintenance.

9.3.1.5. Regulated entities shall ensure that third-parties map personal data storage locations across environments (e.g., on-premise, cloud, mobile) and ensure traceability and compliance with classification labels.

9.3.1.6. Regulated entities shall ensure that third-parties implement role-based access control mechanisms that limit access to personal data based on its classification, and conduct periodic access reviews.

9.3.1.7. Regulated entities shall ensure that third-parties review personal data inventories, ownership, and classification tags on at least an annual basis or upon significant operational changes.

9.3.2 Data Handling

9.3.2.1. Regulated entities shall ensure that third-parties document detailed handling procedures for each classification level, covering storage, transfer, encryption, disposal, and breach escalation steps.

9.3.2.2. Regulated entities shall ensure that third-parties identify and map all cross-border personal data transfers, specifying transfer mechanisms (e.g., SCCs, BCRs) and destination countries per classification.

9.3.2.3. Regulated entities shall ensure that third-parties deploy automated discovery and classification tools capable of scanning repositories, detecting personal data, and tagging it as per policy.

9.3.2.4. Regulated entities shall ensure that each classified personal data item is associated with a documented lawful basis for processing, and this is captured within the data inventory by third-parties.

9.3.3 Awareness on Classification

9.3.3.1. Regulated entities shall ensure that third-parties provide training to relevant staff on the classification policy and proper handling techniques for different categories of personal data, with emphasis on risk mitigation.

10.Sub-Contracting

Overview: This domain shall ensure third-party sub-contracting arrangements are disclosed and approved, maintaining oversight and control to adhere to vendor risk management policies and mitigate associated risks.

10.1 Disclosure of Subcontractor and Approval from Regulated Entities

Objective: To ensure third-parties disclose sub-contracting arrangements and obtain approval, maintaining oversight and adherence to vendor risk management policies.

10.1.1 Disclosure and Approval:

10.1.1.1. Regulated entities shall ensure that the third-parties have the following:

a) Identification of sub-contracting and approval from Regulated entities before utilizing sub-contractors for the active/new/change of scope of service

b) Vendor Risk Management Policy and Procedure

c) Identification of "nth parties"

10.2 Monitoring and Oversight

Objective: To ensure sub-contracting agreements are signed and risk assessments conducted, maintaining oversight and control over sub-contracted vendors.

10.2.1 Sub-contracting Monitoring and Oversight

10.2.1.1. Regulated entities shall ensure that there is a sub-contracting agreement signed with the sub-contracted vendor(s) and the third-parties and risk assessment is performed on them.

11.Exit Strategy

Overview: This domain shall ensure Regulated Entities implement proper exit strategies for third-party engagements, to maintain service continuity and data security.

11.1 Exit Strategy Planning

Objective: To ensure Regulated Entities establish a comprehensive exit plan and process for third-party engagements, while maintaining service continuity.

11.1.1 Exit Plan and Process

11.1.1.1. Regulated entities shall have a process to off-board / de-activate / blacklist third-party engagements, covering different scenarios while ensuring service continuity.

11.1.1.2. Regulated entities shall have a formalized checklist for off-boarding of third-party engagement.

11.1.1.3. Regulated entities shall have the exit/end of agreement/termination clauses in all third-party agreements.

11.1.1.4. Regulated entities shall conduct knowledge transfer session with the third-party to ensure that all information / knowledge base including all process documents are taken over

11.1.1.5. Regulated entities shall take disposal certificate from the third-party post removal / deletion / purging of necessary information from their system, post the data retention period is completed, wherever applicable.

12.Storage of Data

Overview: This domain establishes the protection measures of sensitive data through secure storage practices, supporting compliance and resilience against data loss and unauthorized access.

12.1 Data Storage Security

Objective: To ensure third-parties implement robust security measures to protect sensitive data and prevent unauthorized access or data leakage.

12.1.1 Storage Access and Segmentation

12.1.1.1. Regulated entities shall ensure that third-parties enforce role-based access control (RBAC) for all storage environments, ensuring only authorized personnel can access, modify, or delete data based on job responsibilities.

12.1.1.2. Regulated entities shall ensure that third-parties logically or physically segregate storage locations for different data classifications (e.g., public, internal, restricted) to prevent unauthorized access or data leakage

12.1.1.3. Regulated entities shall ensure that third-parties maintain a comprehensive inventory of all physical and cloud-based storage locations where personal, sensitive, or regulated data resides, including geographic location

12.1.1.4. Regulated entities shall ensure that third-parties restrict use of portable storage (e.g., USB drives, external HDDs) and enforce encryption and tracking mechanisms for permitted devices.

12.1.2 Storage Configuration Management

12.1.2.1. Regulated entities shall ensure that third-parties define and implement baseline configurations for all data storage systems, including permissions, patch levels, and encryption settings.

12.1.2.2. Regulated entities shall ensure that third-parties configure cloud storage services with encryption, access control, activity logging, and data residency compliance in line with organizational security policies.

12.1.2.3. Regulated entities shall ensure that third-parties implement network segmentation to isolate critical storage infrastructure from general corporate networks and reduce the attack surface.

12.2 Storage Lifecycle Management

Objective: To ensure the effective implementation of data retention and deletion policies by third-parties, to comply with legal, regulatory, and operational requirements.

12.2.1 Data Retention

12.2.1.1. Regulated Entities shall ensure that third-parties implement automated mechanisms within storage platforms to enforce retention periods and flag or delete expired data.

12.2.1.2. Regulated entities shall ensure that third-parties securely delete data using methods aligned with best practices (e.g., cryptographic erase, secure wipe) to ensure data cannot be reconstructed.

12.2.1.3. Regulated entities shall ensure data stored in backup repositories by third-parties adheres to the same retention, access control, and encryption policies as primary data stores.

12.2.2 Archival and Purge

12.2.2.1. Regulated entities shall ensure that third-parties define archival policies for inactive or legacy data, ensuring that only essential data is retained and remains accessible when needed.

12.2.2.2. Regulated entities shall ensure that third-parties perform scheduled reviews of stored data and purge non-essential or obsolete records based on data minimization principles.

12.2.2.3. Regulated entities shall ensure that third-parties periodically audit data storage platforms to ensure compliance with the defined retention and deletion policies.

12.2.2.4. Regulated entities shall ensure that third-parties define procedures for data migration across storage platforms, ensuring secure handling, classification preservation, and integrity validation.

12.2.2.5. Regulated entities shall ensure that third-parties periodically evaluate stored data sets to eliminate unnecessary personal or duplicate data in accordance with data minimization obligations.

12.2.2.6. Regulated entities shall ensure that third-parties implement appropriate storage redundancy (e.g., RAID, replication) aligned with criticality and availability needs, ensuring resilience and continuity.

12.3 Data Integrity and Availability

Objective: To ensure continuous data availability and resilience by implementing adequate and reliable backup and recovery procedures, integrity checks, fault tolerance mechanisms, and disaster recovery integration, safeguarding against disruptions and data loss.

12.3.1 Backup and Recovery

12.3.1.1. Regulated entities shall ensure that third-parties establish and test comprehensive backup and restoration procedures for all critical data to ensure data availability and resilience.

12.3.1.2. Regulated entities shall ensure that third-parties implement automated integrity checks (e.g., checksums, hashes) on stored data to detect corruption or unauthorized changes.

12.3.1.3. Regulated entities shall ensure that third-parties deploy storage systems with fault-tolerance features (e.g., failover, replication) to ensure continuous access to critical data even during hardware failure or outages.

12.3.1.4. Regulated entities shall ensure that third-parties define time-bound objectives (RTO/RPO) for restoring access to data in case of disruptions and monitor adherence through simulations and reviews.

12.3.1.5. Regulated entities shall ensure that third-parties use write-once or immutable storage configurations for critical system logs, audit trails, and evidence repositories to prevent tampering or deletion.

12.3.1.6. Regulated entities shall ensure that third-parties integrate storage infrastructure with the enterprise disaster recovery plan to ensure timely and secure restoration of stored data following a major incident.

13.Cross-Border Transaction

Overview: This domain shall establish compliance measures for cross-border transactions, ensuring adherence to legal, regulatory, and privacy requirements to mitigate risks and uphold financial integrity.

13.1 Regulatory & Legal Compliance

Objective: To ensure Regulated Entities conduct cross-border transactions through authorized channels, maintaining compliance with trade regulations, sanctions, screening, and licensing requirements to uphold legal and financial standards.

13.1.1 Transactional Controls

13.1.1.1. Regulated entities shall route cross-border payments exclusively via licensed payment systems recognized by CBK, ensuring full compliance with regulations and cross-border settlement standards (e.g., FSB PFMIs).

13.1.1.2. Regulated entities shall maintain complete documentation, including invoices, bills of lading, and customs entries, as per trade regulations and international norms.

13.1.1.3. Regulated entities shall screen counterparties and transactions against FATF, UN, US, EU, and other internationally recognized sanctions and embargo lists in real time.

13.1.1.4. Regulated entities shall collect and validate valid LEIs for counterparties involved in transactions above defined thresholds, complying with global LEI standards.

13.1.1.5. Regulated entities shall verify that cross-border transactions have the necessary CBK approvals and adhere to foreign exchange control authorizations, corporate licensing, and sector-specific limits.

13.2 Due Diligence & KYC/AML

Objective: To ensure Regulated Entities perform thorough customer identification and due diligence processes for cross-border transactions, adhering to the applicable standards and rules to mitigate risks and ensure compliance.

13.2.1 Due Diligence Process

13.2.1.1. Regulated entities shall perform comprehensive KYC, including identity verification and beneficial ownership checks, prior to initiating cross-border transactions.

13.2.1.2. Regulated entities shall apply risk-based due diligence, considering jurisdictional risk, transaction size, and customer profile, and document all findings accordingly.

13.2.1.3. Regulated entities shall perform enhanced due diligence, including source-of-funds and senior management approval, on PEPs, high-risk countries, or large-value transactions.

13.2.1.4. Regulated entities shall transmit full originator and beneficiary details in accordance with FATF Recommendation 16 (Travel Rule) for all cross-border transfers above applicable thresholds.

13.2.1.5. Regulated entities shall assess and document AML/CFT controls of correspondent banks per FATF and BIS guidance, with periodic updates based on risk.

13.3 Secure Data Transfers & Privacy

Objective: To ensure Regulated Entities manage cross-border transactions securely and compliantly.

13.3.1 Data Minimization and Secure Transmission

13.3.1.1. Regulated entities shall limit cross-border data to only what is strictly necessary and proportionate, in adherence to CBK privacy directives and international data protection frameworks.

13.3.1.2. Regulated entities shall ensure cross-border payment data is transmitted using encrypted methods (e.g., TLS 1.2+, IPsec) and authenticated interfaces.

13.3.1.3. Regulated Entities shall implement legal transfer mechanisms (e.g., SCCs, BCRs), or obtain CBK permissions for data transfers.

13.3.1.4. Regulated Entities shall conduct PIAs or DPIAs for new or high-risk data transfers crossing borders, recording risk assessments and mitigating actions.

13.4 Monitoring, Reporting & Audit

Objective: To ensure Regulated Entities implement robust transaction monitoring, audit logging, and compliance reporting systems for cross-border activities, adhering to AML/CFT standards and regulatory requirements.

13.4.1 Transaction Monitoring & Alerts

13.4.1.1. Regulated Entities shall operate real-time AML/CFT systems to detect unusual cross-border patterns (e.g., volume, frequency, location), generating alerts and case investigations.

13.4.1.2. Regulated Entities shall maintain tamper-evident, time-stamped logs of all transaction workflows, including initiation, approval, messages, and settlement, for a retention period as specified.

13.4.2 Regulatory Reporting Requirements

13.4.2.1. Regulated Entities shall submit cross-border reports (e.g., large transfers, STR/FTR filings, statistical returns) to CBK and affiliated authorities within prescribed timelines.

13.4.2.2. Regulated Entities shall conduct internal or external audits of cross-border compliance controls and submit the resulting findings and remediation plans to CBK.

14.Usage of Cloud Services

Overview: This domain shall ensure Regulated effectively manage the risks associated with cloud service providers, ensuring compliance across jurisdictions, and maintaining cloud security, which is crucial for safeguarding data.

14.1 Cloud Security

Objective: To ensure Regulated Entities implement robust cloud security measures, safeguarding data confidentiality, integrity, availability, and compliance, while managing risks associated with Cloud Service Providers (CSPs).

14.1.1 Cloud Security Safeguards

14.1.1.1. All applicable cloud security controls defined in the Cyber Resilience Baselines shall be evaluated as part of the assessment process.

14.1.1.2. Regulated Entities shall have a record of Cloud Service Provider (CSP) details, locations and type of cloud services used:

a) Public Cloud
b) Private Cloud
c) Hybrid Cloud
d) Community cloud

14.1.1.3. Regulated Entities shall have details of Cloud service model that is being utilized for providing services:

a) Software as a Service (SaaS)
b) Platform as a Service (PaaS)
c) Infrastructure as a Service (IaaS)

14.1.1.4. Regulated Entities shall ensure that all legal and regulatory requirements that apply to the provision and use of cloud services are identified. Particularly where the processing, storage and communication capabilities are geographically distributed and multiple jurisdictions are involved.

14.1.1.5. Regulated Entities shall ensure that the Cloud Service Provider is a Cloud Security Alliance Security, Trust and Assurance Registry (“STAR”) certified provider or holds a cloud-based certification (i.e., ISO 27017, FedRAMP).

14.1.1.6. Regulated Entities shall ensure that security control ownership is clearly defined in a shared security responsibility model between CSP and RE and documentation is available.

14.1.1.7. Regulated Entities shall have strategies in place to mitigate the risk of vendor lock-in with the cloud service providers and have measures related to data portability, use of open standards, and multi-cloud strategies etc.

14.1.1.8. Regulated Entities shall ensure that CSP provide a third-party audit report i.e., SOC 2 Type II report / ISAE 3402 report or equivalent.

14.1.1.9. Regulated Entities shall ensure that procedures are in place to ensure the secure termination of services and data retrieval when the agreement ends.

14.1.1.10. Regulated Entities to ensure that the CSP have the capabilities to enable them to monitor activity within a cloud computing environment.

15.Inter-Affiliates

Overview: This domain shall establish the requirements for managing affiliate engagements in an effective way to uphold compliance, mitigate risks, and maintain services continuity.

15.1 Due Diligence and Periodic Review

Objective: To ensure Regulated Entities maintain effective monitoring and oversight of affiliate engagements through defined due diligence processes.

15.1.1 Inter-Affiliates Monitoring and Oversight

15.1.1.1. Regulates Entities shall define the scope of due-diligence on affiliates, have Service Level Agreements (SLAs) in place, perform periodic reviews and have an exit strategy in place.

15.1.1.2. Regulates Entities shall seek prior approval from the CBK before entering material or high-risk service arrangements with affiliates. Regulated Entities shall ensure robust risk assessment, governance, and compliance with regulatory requirements for all affiliate services, and seek approval where such arrangements could impact the entity's risk profile or operational resilience.

15.2 Customer Consent

Objective: To ensure the implementation of a customer consent procedure for data sharing with affiliates.

15.2.1 Customer Consent for Data Sharing

15.2.1.1. Regulated Entities shall ensure to have a customer consent procedure in the case of data sharing with the affiliates.

15.3 Foreign Affiliates

Objective: To ensure the application of consistent controls and governance for foreign affiliates, considering geopolitical relations.

15.3.1 Foreign Affiliates

15.3.1.1. Regulated entities shall ensure similar controls and governance are adhered to in the case of foreign affiliates apart from considering geo-political relations between countries.

15.4 Resource Planning

Objective: To ensure Regulated Entities effectively plan and allocate resources to maintain service viability and continuity.

15.4.1 Business Continuity

15.4.1.1. Regulated entities shall ensure resource planning and availability to ensure service viability.

16.Exceptions Under the CORF

Any exception or exemption to one or more controls outlined in this Third-Party Risk Management Baselines requires regulated entity to submit a formally justified exception request, including proposed compensating controls. This request shall be submitted to the Central Bank of Kuwait (CBK) for evaluation and approval before any exception or exemption can be granted.

17.Appendix – Terms and Definitions

Term	Definitions
Asset	An asset (tangible or intangible) is any resource or item of value owned or controlled by a Regulated Entity that can be used to achieve its objectives.
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

Term	Definitions
Compliance Requirements	Global regulations, national and international laws, regulatory requirements, applicable technology standards, and guidelines provided by leading service providers.
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.
Electronic Records / Information	Records maintained by the entity in electronic form.
Emerging Technologies	Innovative advancements in their early stages of development or adoption, with potential to significant impact on industries by transforming operations, enhancing security, and reshaping traditional services, enabling new business models, improving efficiency, and providing competitive advantage. Examples include AI, ML, Cloud, Blockchain, IoT, 5G, and quantum computing.
Foreign-Affiliates	Affiliated entities located outside the organization's home jurisdiction, such as foreign subsidiaries, branches, or joint ventures. These entities operate under different legal, regulatory, and operational frameworks, and may be subject to local compliance, reporting, and governance requirements.
Inter-Affiliates	Entities within the same corporate group, including parent companies, subsidiaries, or sister entities, that engage in operational, financial, or service-related transactions. These relationships may involve shared infrastructure, personnel, or resources, and are typically governed by internal agreements or group policies.
Important Records	Electronic records of the nature of transactional data, sensitive and personally identifiable information processed by the regulated entity.

Term	Definitions
Information Processing Facilities	A physical location which hosts information processing systems, services or technology assets.
Information Asset	Data, information, or knowledge that is valuable to an organization and is stored, processed, or transmitted in any form. This includes electronic data, documents, databases, software, and any other information resources that support business operations and decision-making.
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	Refers to any electronic device that is portable and have the capability to store, transmit, and/or process data, whether it is owned by the Regulated Entity or employees and are allowed to connect to the Regulated Entities network. Examples include -but not limited to- laptops, mobile devices.
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 Executive/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.

Term	Definitions
Significant Third-Party Agreements	A significant third-party agreements refers to any third-party arrangement that in the event of failure impacts the operations, service to customers, data privacy, financial stability, and legal and regulatory compliance. This includes g) Core or critical business functions essential to the Entity's operations and delivery of services to customers; h) Access to or processing of sensitive data, including personal or financial data and information; i) Outsourcing of cybersecurity monitoring and response activities, such as Security Operations Center (SOC), and other similar activities that are critical to the Entity's ability to detect and mitigate threats; j) IT infrastructure hosting, platform and cloud services that support critical systems, databases, and applications; k) Payment processing, transaction management, and other related services essential to the business and customer access to financial services; and l) IAM services or other security operations that manage access and encryption to critical systems and data.
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.

18.Appendix - Glossary

Term	Definition
CBK	Refers to the “Central Bank of Kuwait”.
CORF	Refers to the “Cyber and Operational Resilience Framework”.
Banking and Financial Sector and Other CBK Regulated Entities	Refers to CBK and all entities that are regulated by CBK including Local Banks, Foreign Banks, Exchange Companies, Payment service providers, Open Banking Service Providers, and other regulated Finance Companies.
Kuwaiti banks	Refers to banks that have Kuwaiti promoters including Islamic, Conventional, and specialized banks.
Foreign banks	Foreign Banks in the state of Kuwait that are authorized by CBK.
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 ● E-Payment of Funds Companies ● Credit Information Companies ● Open Banking Service Providers
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 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.
TPRM maturity	Refers to the assessment of third-party risk management against levels defined as a part of the third-party risk assessment process.
ISO/IEC	International Organization for Standardization/ International Electrotechnical Commission