Central Bank of Trinidad & Tobago

# A Report on the Thematic Review of Commercial Banks' Cybersecurity Risk Management Practices

August 2022

## Table of Contents

# 1 EXECUTIVE SUMMARY

## 1.1 Preface

This report sets out the key findings from a thematic review of commercial banks' cybersecurity risk management practices, which was conducted by the Central Bank of Trinidad and Tobago ("Central Bank"/ "Bank") over the period January 2020 – March 2022. The commercial banking sector in Trinidad and Tobago comprises eight commercial banks, of which five are foreign owned and three are locally owned banks.

Cyber risk[1] means any risk of financial loss, disruption, or damage to the reputation of an organization from potential failure of its information technology systems, while cybersecurity[2] is the art of protecting networks, devices, and data from unauthorized access or criminal use, and the practice of ensuring confidentiality, integrity, and availability of information. With the increasing advancement of digital technology, banks have enhanced the offer of online banking services to their customers. Virtualization and digitization have increased the accessibility of online banking services however; the banking applications and devices on the network used for such services are now even more prone to cyber-attacks. Consequently, to resolve such occurrences, the implementation of an appropriate cybersecurity framework has become critical to mitigate the risk of cyber-attacks.

Due to the onset of the Covid-19 pandemic ("pandemic"), the onsite exercise, which commenced just prior to the start of the pandemic, was suspended. The Bank subsequently resumed the thematic review in April 2021 as a combined virtual / desk-based examination. Virtual interviews were conducted with key personnel and a desk-based review of documentation was completed to determine the existence and suitability of the cybersecurity controls at the commercial banks. The review did not include the testing of controls and processes to allow for an evaluation of effectiveness. This thematic review was a key deliverable on the Central Bank's Strategic Plan.

## 1.2 Scope and Objectives of the Thematic Review

The scope of the thematic review of the cybersecurity risk management practices covered seven of the eight commercial banks[3] operating in Trinidad and Tobago, which focused on the following **six** key objectives:

---

1 https://www.theirm.org/what-we-say/thought-leadership/cyber-risk/#:~:text='Cyber%20risk'%20means%20any%20risk,of%20its%20information%20technology%20systems.

2 https://www.cisa.gov/uscert/ncas/tips/ST04-001

3 For the purposes of the report, commercial banks will be referred to as "banks" or "financial institutions" interchangeably throughout the document. One small commercial bank was omitted from the scope of the exercise as it was in the process of changing out its information technology systems. The findings in this report will not be impacted by this commercial bank's omission from the exercise.

i. Adequacy of the cybersecurity governance framework in relation to the technological complexity of the institution;
ii. Adherence of the financial institution ("FI") to its own cybersecurity policies and practices;
iii. Adequacy of cybersecurity monitoring and systems that institutions utilise in order to mitigate cybersecurity risks;
iv. Quality of the processes for response and recovery;
v. Adequacy of the processes implemented for continuous learning of the cybersecurity landscape and the financial institution's role in cybersecurity information sharing within the sector; and
vi. Determination on whether cyber resilience is being managed in accordance with international best practices, as well as, the Central Bank's Guidelines on Corporate Governance ("CGG"), Security Systems for Safeguarding Customer Information ("SSG"), and Market Conduct for Licensees under the Financial Institutions Act, 2008 ("MCG").

The thematic review was aligned with the Federal Financial Institutions Examination Council's ("FFIEC") 2017 Cybersecurity Assessment Tool (CAT), which consisted of two parts; (1) an Inherent Risk Profile, which was determined by each commercial bank's self-assessment of its inherent risk, and (2) a Cybersecurity Maturity assessment. In the context of the thematic review, notable divergences between the entity's inherent risk profile, and the expected cybersecurity maturity level of that entity's cybersecurity environment was considered a gap.

There are **five** domains in FFIEC's assessment tool, which covered Cyber Risk Management and Oversight; Threat Intelligence and Collaboration; Cybersecurity Controls; Management of External Dependency; and Cyber Incident Management and Resilience. These domains are explained and assessed in sections 2 to 7 of this Report.

The six objectives of the thematic review were analysed using the five domains listed above to complete the assessment of cyber risk at the banks, which yielded the following key observations detailed below.

## 1.3 Key Observations

- The gaps identified between different commercial banks within the sector were largely related to the non-existence or unsuitability of controls, and were based on their maturity levels, sizes, and ownership structures.
- In most cases, commercial banks featured some centralized cybersecurity oversight functions but with individual business units or entities given execution capabilities.

- For foreign owned banks, the management of the information security and services between the parent and local subsidiary was governed by a contractual agreement, which resulted in information security and cybersecurity services being driven by the parent, with limited activities being performed by local employees who support the information security team of the parent entity.
- Generally, commercial banks maintained cyber risk governance frameworks and cyber risk management practices that were developed and implemented in accordance with international frameworks and standards (e.g. ISO27001, NIST CSF, CIS Security Controls, COBIT 2019).
- Banks commonly applied the three lines of defense model. Oversight and management of cyber risk included a cascading responsibility structure with defined roles, appropriate reporting lines, specialized information security or cybersecurity units, and a hierarchy of authority.
- Generally, commercial banks engaged a managed security services provider (MSSP)[4] or operated a 24x7 Security Operations Center (SOC)[5] to provide a range of activities. Key activities included, threat identification and assessment, which dealt with the collection, analysis and monitoring of cyber threats outside the banks, as well as, incident detection and management, to detect, identify, investigate, and respond to cyber incidents.
- Based on a review of strategies, initiatives, and budgets, there was evidence to suggest that commercial banks made efforts to direct greater attention to cybersecurity risk management.

## 1.4 Key Areas that Warrant Attention

While in general, commercial banks appeared to have fairly robust cyber security frameworks in place, there are a few areas that warrant attention as follows:

- Three of the seven commercial banks did not have a clearly documented and board approved information security strategy.
- Two commercial banks were tardy concerning the regular review and updating of their Information Security Policies and Procedures.

[4] A **managed security service provider (MSSP)** provides outsourced monitoring and management of security devices and systems. MSSPs use security operation centers to provide 24/7 services designed to reduce the number of operational security personnel an enterprise needs to hire, train and retain to maintain an acceptable security posture.

[5] **Security Operations Center (SOC)** is a centralized function or service responsible for detecting, analyzing, and responding to cybersecurity incidents in a timely manner. The purpose of the SOC is to defend and monitor an organization's systems and networks (i.e., cyber infrastructure) on an ongoing basis.

- The processes for the management of cybersecurity risk at three commercial banks did not include measures to monitor cybersecurity risks against their approved risk appetites, or to report cybersecurity risks that exceeded their risk appetites.
- Half of the commercial banks did not provide information security awareness training that was customized towards their users' job functions. As a result, high-risk groups such as those with privileged accounts did not receive training commensurate with their levels of responsibility.
- There was no formal evidence of threat information sharing among the commercial banks within the sector, to facilitate access to threat information that might otherwise be unavailable to individual entities, as well as, to enhance their security posture by leveraging the knowledge, experience, and capabilities of their partners in a proactive way.[6]
- Three commercial banks externally sourced cybersecurity functions from the same managed security service provider, which raised a potential concern of concentration risk[7].
- Areas for improvement were required in the management of three commercial banks' external dependency, particularly, in regard to the lack of inclusion of key provisions in contracts as well as underdeveloped ongoing monitoring practices.

6 Source [NIST Special Publication 800-150 - Guide to Cyber Threat Information Sharing].
7 "Concentration risk" in this context refers to the potential system risks posed where outsourced activities of multiple regulated entities are concentrated in a single third party service provider.

# 2 INTRODUCTION

Cyber incidents pose risk to financial institutions and to financial stability. The increasing frequency and severity of cyber threats and use of digitalisation of financial products and services lead to the Central Bank's commencement of a thematic review of Cybersecurity Risk Management Practices ("thematic review") in the banking sector that commenced in 2020, just prior to the start of the pandemic.

The thematic review was conducted across seven of the eight commercial banks to gather information on their cybersecurity framework/practices and cyber resilience. The pandemic impacted the manner in which the Central Bank was able to progress the onsite review of cyber risk, due to the implementation of government's public health protocols that restricted the Bank's ability to visit financial institutions and conduct physical onsite examinations.

Consequently, the Bank adopted an alternative approach, and first requested the financial institutions to complete a workbook based on the Federal Financial Institutions Examination Council ("FFIEC") Cybersecurity Assessment Tool ("CAT"). The banks were also asked to submit electronically key policy documents related to cyber risk management to the Central Bank for review. The Bank's assessment then commenced with a review of the responses from the assessment tool and an off-site review of the documents submitted by the financial institutions. The second part of the assessment involved a conduct of virtual interviews with key personnel from the financial institutions, including Information Technology ("IT") staff, members of their Audit Committees, as well as, the Internal Auditor. The off-site team placed heavy reliance on the institutions' assessments of the complexity of their technological and business operating environments, and their responses to the questionnaire.

## 2.1 Assessment Methodology

The thematic review was aligned with the Federal Financial Institutions Examination Council's ("FFIEC") 2017 Cybersecurity Assessment Tool (CAT), which consisted of two parts; (1) an Inherent Risk Profile, which was determined by each commercial bank's self-assessment of its inherent risk, and (2) a Cybersecurity Maturity assessment. In the context of the thematic review, notable divergences between the entity's inherent risk profile, and the expected cybersecurity maturity level of that entity's cybersecurity environment was considered a gap. There are **five** domains in FFIEC's assessment tool, which covered Cyber Risk Management and Oversight; Threat Intelligence and Collaboration; Cybersecurity Controls; Management of External Dependency; and Cyber Incident Management and Resilience. The respective domains cover the following areas:-

- **Domain 1** covers the adequacy of **Cyber Risk Management and Oversight**, which addresses the board of directors' (board's) oversight and management's development and implementation of an effective enterprise-wide cybersecurity program with comprehensive policies and procedures for establishing appropriate accountability and oversight. It also includes the allocation of the FI's resources for cyber risk, as well as, training and culture.
- **Domain 2** captures the quality of **Threat Intelligence and Collaboration**, which includes processes to effectively discover, analyze, and understand cyber threats, with the capability to share information internally and with appropriate third parties. It also incorporates monitoring and analysis, as well as, information sharing.
- **Domain 3** looks at the adequacy of **Cybersecurity Controls**, which are the practices and processes used to protect assets, infrastructure, and information by strengthening the institution's defensive posture through continuous, automated protection and monitoring. It includes preventative controls, detective controls, and corrective controls.
- **Domain 4** reviews the quality of the **Management of External Dependency**, which involves establishing and maintaining a comprehensive program to oversee and manage external connections and third-party relationships with access to the institution's technology assets and information.
- **Domain 5** looks at the adequacy of **Cyber Incident Management and Resilience**, which includes establishing, identifying, and analyzing cyber events; prioritizing the institution's containment or mitigation; and escalating information to appropriate stakeholders. Cyber resilience encompasses both planning and testing to maintain and recover ongoing operations during and following a cyber-incident.

The six objectives of the thematic cyber risk review of the commercial banks were analysed using the five domains listed above. The assessment of each of the domains 1 thru 5 is covered in sections 3 to 7 of this Report, respectively.

# 3 CYBER RISK MANAGEMENT AND OVERSIGHT

## 3.1 Board Oversight and Strategy

- Commercial banks' governance models for cyber risk generally involved a Board of Directors or appropriate Board Committee, with responsibility for ensuring that information security and cybersecurity policies were developed, implemented, and maintained. Committees of the Board are charged with direct oversight of the commercial banks' cyber risk management practices as well as the cybersecurity program's general progress. However, it was noted that **three of the seven commercial banks did not maintain a documented information security strategy**, the purpose of which was to outline the initiatives/action plans, required resources, training, and goals to improve their institution's cybersecurity capabilities and mitigate risk.

## 3.2 Policies and Procedures

- Information security or cybersecurity policies and procedures for most commercial banks were commensurate with their risk and complexity. These policies and procedures were generally comprehensive, and addressed the concepts of information security risk management, third party risk management, as well as, incident response and resilience. It was noted, however, that two of the commercial banks' policies and procedures were not updated in line with their proposed review cycles.

## 3.3 Cybersecurity Budget

- Generally, commercial banks conducted their cybersecurity budgeting process on an annual basis. These budgets related to the development, implementation, and maintenance of a successful information security programme. Some commercial banks' cybersecurity budgets were subsumed in their IT budget, whilst other banks maintained a specific budget targeted towards cybersecurity. For most banks, the cybersecurity budget has been increasing annually.

## 3.4 Cybersecurity Reporting

- Cybersecurity related reports were usually provided to an appropriate Board Committee or Management Committee. Some commercial banks employed the monitoring services of an MSSP, through which cybersecurity reporting was largely provided. Commercial banks also indicated that the information being reported by the MSSP was adequate.

## 3.5 IT Asset Management

- Commercial banks maintained an inventory of technology assets, classified by their sensitivity and criticality. This inventory included hardware, software, and information assets. Policies related to the governance of the inventory;

classification of assets both at inception and throughout the asset life cycle; and the periodic update to ensure accuracy; were observed and considered adequate.

### 3.6 Risk Management and Assessment

- All commercial banks maintained enterprise wide risk management policies and procedures that have been approved at the board level. Comprehensive risk assessment processes were in place to identify internal and external security threats and evaluate the potential impact and consequences of the threats and vulnerabilities on the business and operations. **However, it was noted that the processes for the management of cyber risk for some commercial banks did not include measures to monitor cybersecurity risks against the approved risk appetite, or to report cybersecurity risks that exceeded the risk appetite**.

### 3.7 Internal Audit

- Internal audit represented the third line of defence and provided objective assurance on the effectiveness of the commercial banks' cyber risk management and internal controls. Internal Audit reported directly into the Audit Committee on the results of their cyber reviews. The Audit Committee also provided an additional layer of oversight, to ensure control weaknesses were addressed in compliance with cybersecurity policies.

### 3.8 Resources

- For all commercial banks, the maturity of their cybersecurity capabilities was influenced by the extent to which they had support from regional or international parents and/or partner entities. The foreign owned banks in particular, leveraged the expertise and resources of their global and regional parents to support their cybersecurity programs. The other commercial banks experienced capacity and resource constraints. In these cases, third party service providers were used to supplement technical and managerial capabilities.

### 3.9 Training

- Six of the seven commercial banks provided training to the Board and Board Committee members to raise their awareness on the latest cyber security landscape. It was also noted that six of the seven commercial banks provided annual mandatory information security and awareness training as well as ongoing security-related communications to employees to develop and maintain awareness of, and competencies for, detecting and addressing cyber-related risks. Generally, training programs included scenarios capturing areas of significant and growing concern, such as phishing attempts. However, it was noted that at 50% of the commercial banks, the training provided was not consistent with the level of risk associated with users' functions or roles. Consequently, **high-risk groups,**

**such as those with privileged account permissions, did not usually receive additional information security training commensurate with their levels of responsibility**.

# 4 THREAT INTELLIGENCE AND COLLABORATION

## 4.1 Threat Intelligence

- Commercial banks established a threat intelligence process to gather and analyse relevant cyber threat information to assist management in its identification of information security risks. While generally the threat intelligence process implemented by the commercial banks was considered adequate, some commercial banks lacked more enhanced capabilities such as **threat modelling**[8] to better understand the nature, frequency, and sophistication of threats; to evaluate the information security risks specific to the institution; and to apply this knowledge to the institution's information security program.

## 4.2 Monitoring and Analysis

- Generally, commercial banks had processes in place to continuously monitor threats and vulnerabilities relevant to their business processes, which sometimes involved the use of an MSSP. The roles and responsibilities for monitoring threats were also clearly defined. A process to review and retain audit log records and other security event logs had been established to facilitate commercial banks' security monitoring operations and enable a proactive readiness within the entities to mitigate risks.

## 4.3 Information Sharing

- Six of the seven commercial banks belong or subscribe to a threat and vulnerability information sharing source. Information about threats generally came from government (e.g., US-CERT[9], TT-SCIRT[10]), information-sharing organizations (e.g., Financial Services Information Sharing and Analysis Center - FS-ISAC), industry sources, or other third parties.

- All commercial banks gathered and shared information security threat data with applicable internal employees. It was however, noteworthy **that there was a lack of threat information shared amongst banks locally**. Responses indicated that this was due to the absence of formal information sharing structures designed to provide assurances of trust and confidentiality required for threat information sharing across organizational boundaries. The non-existence of a legislative

[8] Threat modelling is a structured approach that enables an institution to aggregate and quantify potential threats.
[9] U.S. Computer Emergency Readiness Team
[10] T&T Cyber Security Incident Response Team

framework for sharing information to define what information is to be shared, with whom, and for what purposes, was also mentioned.

# 5 CYBERSECURITY CONTROLS

- Generally, commercial banks have implemented protective, detective, and corrective controls that align security with the institutions' operations and cybersecurity strategies. Controls included, but were not limited to; patch management, asset and configuration management, vulnerability scanning and penetration testing, end-point security, resilience controls, logging, and monitoring.

## 5.1 Preventative Controls

- Most commercial banks implemented appropriate protective controls in line with industry standards, to minimise the likelihood and/or impact of a cyber-attack on identified critical business functions, information assets, and data. Protective controls were directly related to each commercial bank's threat landscape and systemic role in the financial system.

- Protective controls were also implemented to ensure the security of information within commercial banks' environments, including their networks and connected services. It was noted that commercial banks' infrastructures were protected through controls around configuration and patch management, privileged access, and segregation of duties. The use of perimeter devices and systems to prevent and detect unauthorized access was also noted. The most common approaches used to enforce and detect perimeter protection included, inter alia, router configurations, firewalls, Intrusion Prevention Systems (IPS), Data Loss Prevention (DLP) systems, and Distributed Denial of Services (DDoS) mitigating technologies.

- Commercial banks implemented measures, such as encryption and multifactor authentication, to protect information, both in transit and at rest, commensurate with the criticality and sensitivity of their data. Of note, was the consideration of one commercial bank, for the use and implementation of quantum cryptography[11]

- Access rights at commercial banks' were granted in accordance with each institution's physical and logical access control policies or standards. Generally, it was observed that commercial banks' employee access was role-based, provided

[11] Quantum cryptography is a method of encryption that uses the naturally occurring properties of quantum mechanics to secure and transmit data in a way that cannot be hacked. Cryptography is the process of encrypting and protecting data so that only the person who has the right secret key can decrypt it.

for separation of duties, and granted on the principles of least privilege, which recommends minimum user profile privileges for both physical and logical access based on job necessity.

### 5.2 Detective Controls

- Commercial banks established capabilities to continuously monitor and detect anomalous activities and events. Generally, the commercial banks' cybersecurity detective controls were adequately designed to mitigate cyber threats and these controls were observed to be generally managed or performed by a Security Operations Center (SOC), operated either internally or by an external party.

- Six of seven commercial banks conducted annual penetration testing, which is a specialized type of assessment conducted on systems or individual system components to identify vulnerabilities that could be exploited by adversaries. It was noted that three banks with more mature security programs, employed red team exercises[12], to simulate attempts by adversaries to compromise mission and business functions, and provide a comprehensive assessment of the security and privacy posture of systems within the organization.

### 5.3 Corrective Controls

- Commercial banks established and implemented a patch management process that identifies and ensures software patches are prioritized and implemented within a timeframe that is commensurate with the criticality of the patches and the banks' IT systems. Their patch management processes also included the testing of patches before they were applied to their IT systems in the production environment.

## 6 EXTERNAL DEPENDENCY MANAGEMENT

### 6.1 Relationship Management

- Five of the seven commercial banks have developed and implemented a comprehensive outsourcing or third party risk management policy or framework, commensurate with the nature, scope, and complexity of their outsourcing arrangements.

- Three of the seven commercial banks with challenges related to the capacity or capability of their information security teams sourced some cybersecurity functions externally. The most prevalent outside support was with one particular

[12] Red team exercises extend the objectives of penetration testing by examining the security and privacy posture of organizations and the capability to implement effective cyber defences.

MSSP that provided services such as, 24*7 monitoring, log aggregation, and vulnerability management. This raises a concern of concentration risk[13].

- Third party relationship management for most commercial banks included due diligence, adequate contracts, and ongoing monitoring to help ensure that the services provided were in line with the contractual arrangements. However, **it was noted that three commercial banks' contracts with third-party providers did not include key provisions, which stipulated a review and validation of third party security controls by an independent party, as well as, provisions to facilitate the commercial bank's access to those third party reports**. It was also noted that two commercial banks' ongoing monitoring practices required improvement. Examples included: no measures in place to monitor the performance of the service provider, and no regular updates of third party risk assessments.

### 6.2 Connections

- Commercial banks often facilitated remote network connectivity for third party service providers. Generally, commercial banks had processes in place to document third party connections and indicated that steps were taken to ensure that the connection was encrypted and secured. Generally, commercial banks connected to third parties via a dedicated leased line or Virtual Private Networks (VPNs) and monitored and tested controls for primary and backup third party connections on a regular basis.

## 7 CYBER INCIDENT MANAGEMENT AND RESILIENCE

### 7.1 Detection, Response, and Mitigation

- Generally, incident response programs were considered adequate. Commercial banks established and maintained incident response plans and playbooks that provided well-defined, organised approaches for responding to security incidents. It was observed that their general process flow when responding to security incidents included multiple phases, consisting of Event Detection, Analysis/Investigation, Containment, Eradication & Recovery, and Post-Incident Activities/Lessons Learnt.

- All commercial banks maintained a formalized response program with the creation of an incident response team or crisis management team typically responsible for handling, managing, and supporting responses to security incidents. Six commercial banks' response teams included individuals with a wide

[13] "Concentration risk" in this context refers to the potential system risks posed where outsourced activities of multiple regulated entities are concentrated in a single third party service provider.

range of backgrounds and expertise, from several different areas within the institution. These included Legal, Compliance, Public Relations, IT and Cybersecurity, and this allowed the commercial banks to handle the wide range of technical and non-technical issues posed by an incident.

- Commercial banks implemented systems to alert, detect, and respond to cyber incidents that could impact the bank's infrastructure, services, and customers. Four banks operated a 24x7 Security Operations Center (SOC) and generally used Security Information and Event Management (SIEM) systems to collect, aggregate, analyse, and correlate information from discrete systems and applications in order to discern trends and identify potential cyber incidents. Some commercial banks also engaged a MSSP to perform log aggregation and correlation services to detect cyber incidents.

### 7.2 Incidence Resilience Planning, Strategy and Testing

- Six commercial banks periodically tested the incidence response program using scenario-based exercises, such as tabletop exercises, to validate the effectiveness of their institution's response and recovery. It was observed that the exercises typically involved relevant internal and external parties, depending on the exercise objectives.

### 7.3 Escalation and Reporting

- Commercial banks had a communication process in place to contact personnel who are responsible for analysing and responding to an incident. Six commercial banks had an established list of internal and external stakeholders to be informed depending on the severity of the incident, and processes to notify regulators of material incidents that may affect the institution's operations, reputation, or sensitive customer information.

## 8 CONCLUSIONS

Considering all the findings from the desk-based thematic cyber review, it was determined that generally:

- the commercial banks adhere to international best practice and the provisions in the various Central Bank guidelines regarding cyber resilience (see section 9 on Recommendations);
- the cybersecurity governance frameworks at commercial banks were adequate relative to their technological complexities. Foreign owned banks' cybersecurity frameworks were found to be more mature than locally owned banks;
- the commercial banks adhered to their own cybersecurity policies and practices;

- the commercial banks' cybersecurity monitoring and systems used to mitigate cybersecurity risks were adequate. However, concerns remained regarding the use of one MSSP by several institutions to provide services such as, 24*7 monitoring, log aggregation, and vulnerability management;
- commercial banks' response and recovery processes were considered adequate;
- commercial banks' processes for continuous learning were evident with ongoing training programmes for information security. There is however the need to develop additional training for high-risk groups who maintain privileged account permissions;
- there was a need to establish a formal structure amongst banks for the sharing of cybersecurity information within the sector.

## 9 RECOMMENDATIONS

The Central Bank assessed the identified gaps observed in the five domains against the best practices espoused in cyber security standards as well as requirements in the Bank's Guidelines. Accordingly, the following detailed recommendations contained in the table below are made to strengthen the commercial banks' cyber security frameworks.

It should be noted that in addition to this Thematic Report, which will be issued to the banks and published on the Central Bank's website, individual feedback letters will be issued to each of the commercial banks that participated in the review.

| Key Findings | Central Bank Guidelines / Best Practice | Recommendations |
|---|---|---|
| **1) Cyber Risk Management and Oversight** | | |
| **Cybersecurity Strategy** – There was no evidence of a clearly documented and board approved information security strategy at some commercial banks. | Section 3.2.2 of the Central Bank's Guideline on Security Systems for Safeguarding Customer Information ("SSG"), states that:<br>The Board of each institution or an appropriate Board committee shall be responsible for: -<br>• Approving the written information security programme;<br>• Setting policy for overseeing the development of and reporting on the implementation and maintenance of the information security programme, including assigning specific responsibility for its implementation and maintenance; and | Financial institutions must ensure that a formal information security /cybersecurity strategy is developed, which identifies the vision/goals, supported by action plans and the required resources and training. The Board must approve the strategy.<br><br>Financial institutions must establish and employ processes to facilitate adequate oversight of the implementation of the strategy by performing the following:<br>• Annually reviewing the documented cybersecurity strategy, with amendments |

| Key Findings | Central Bank Guidelines / Best Practice | Recommendations |
|---|---|---|
| | • Reviewing management's status reports on the security programme within an agreed timeframe. | being approved by the board or designated board committee; and<br>• Quarterly status updates on the strategy implementation submitted by senior management to the Board or designated board committee. The report should incorporate any significant related matters, such as summaries of budget expenses, third party service provider arrangements, testing results, information security training and recommendations for amendments to the strategy. |
| **Policies and Procedures –** Some commercial banks were tardy with regards to the regular review and timely updating of the information security policies.<br><br>Information security policies and procedures are the backbone of an organization and the foundation of a good security program. Failure to update these policies may result in the document being outdated and create inconsistencies between best practices and actual operations. It may also potentially open the door and welcome vulnerabilities from outside threat actors as well as insider threats due to misinformed employees. | Section 3.3.1 of the SSG states that management is responsible for developing and documenting an operating manual of the policies, procedures, and processes of the information security programme.<br><br>Additionally, section 7.2.6 of the Central Bank's Corporate Governance Guideline ("CGG") states that, the Board must ensure that the institution has documented policies and procedures that define activities in accordance with the approved business strategy. | Financial institutions must implement systems to ensure that information security policies are updated and approved and the review cycle is adhered to for the timely review and update of policies. |
| **Risk Management and Assessment** – At some | Section 8.5(d) of the Corporate Governance Guideline (CGG) states | Financial institutions should implement appropriate measures |

| Key Findings | Central Bank Guidelines / Best Practice | Recommendations |
|---|---|---|
| commercial banks, there was little to no evidence of measures to monitor cybersecurity risks against the approved risk appetite, or to report cybersecurity risks that exceeded the risk appetite | that the risk management function should include ongoing objective monitoring of the risk-taking activities and risk exposures in line with the Board approved risk appetite. | to monitor cybersecurity risks against the approved risk appetite and report on the IT and cybersecurity risks that exceed the approved risk appetite. |
| **Training** – At some commercial banks, high-risk groups, such as those with privileged account permissions, did not receive additional information security training commensurate with their levels of responsibility. | According to the National Institute of Standards and Technology (NIST)[14], high-risk groups, such as those with privileged system access or in sensitive business functions, should be identified and should receive targeted information security training.<br><br>Additionally, section 6.2 of the SGG, states that employees should be properly trained in maintaining the security, confidentiality and integrity of customer records and information. Training should be consistent with the user's function. | Financial institutions should develop its cybersecurity training and awareness programme to incorporate additional cybersecurity training to employees with privileged account permissions commensurate with their levels of responsibility. |
| 2) **Threat Intelligence and Collaboration** | | |
| **Information Sharing** – There was no evidence of sharing threat information amongst the commercial banks. | According to the NIST[15], allowing "one organization's detection to become another's prevention" is a powerful paradigm that can advance the overall security of organizations that actively share threat information. | In the absence of legislative requirements or formal structures, financial institutions should consider forming an informal, open, self-organized group that largely operates through voluntary cooperation, where members publish threat information to the group on a voluntary, ad hoc basis and are individually responsible for ensuring that the content provided to the group is suitable for sharing. |

[14] NIST Special Publication 800-50 - Building an Information Technology Security Awareness and Training Program Oct, 2003
[15] NIST Special Publication 800-150 - Guide to Cyber Threat Information Sharing Oct 12, 2020

| Key Findings | Central Bank Guidelines / Best Practice | Recommendations |
|---|---|---|
| **3) External Dependency Management** | | |
| **Relationship Management** - Some commercial banks externally sourced cybersecurity functions from the same MSSP. | According to the Central Bank's Guideline for the Management of Outsourcing Risks, financial institutions should be cautious about outsourcing services from a service provider that supplies services to multiple entities as operational risks are correspondingly concentrated and may pose a systemic threat. | The Central Bank will continue to monitor and consider the potential systemic risks posed where outsourced activities of multiple regulated entities are concentrated in a third party service provider. |
| **Relationship Management** - some commercial banks' contracts did not include key provisions, mainly those stipulating that third party security controls should be reviewed and validated by an independent party with the bank having access to the reports | Section 5.3.1 of the Central Bank's Guideline for the Management of Outsourcing Risks requires proper monitoring and control of the outsourced activity or service. Material outsourcing contracts should include provisions, which allows the financial institution the right to monitor and conduct periodic reviews to verify that the service provider is in compliance with the terms of the contract, or alternatively, to cause an independent auditor to evaluate, on its behalf, the service provider's internal control environment and risk management practices. The contract should also allow the financial institution, in specified circumstances, access to internal and external audit reports prepared on the service provider in respect of the outsourced activity, function, process or service | Financial institutions should broaden the requirements of third party contracts to include at minimum, provisions which allow third party security controls to be independently evaluated by the institution or an independent auditor on its behalf, with the institutions having access to the reports. |
| **Relationship Management** – There were no measures in place to monitor the performance of the service provider and third part risk assessments were not regularly updated. | Section 5.4.3 of the Central Bank's Guideline for Management of Outsourcing Risks requires financial institutions to monitor the service provider's performance and compliance with its contractual obligations as part of their ongoing due diligence of service providers. | Financial institutions must develop their Outsourcing Frameworks to incorporate as part of their on-going monitoring of the third party relationships:<br>• Processes to ensure third party risk assessments are regularly updated; and |

| Key Findings | Central Bank Guidelines / Best Practice | Recommendations |
|---|---|---|
| | | • Measures to monitor the performance of third parties on a continuous basis. |