EXECUTIVE SUMMARY

Cybersecurity risk is embedded in the CBB's supervisory framework, but additional enhancements are needed to formalize guidance and develop more intensive supervisory practices. Supervisory expectations on cybersecurity are presented in an informal guidance note, which should be formalized into regulation to ensure enforceability; and an IT/cybersecurity supervisory manual should be developed to promote effective and consistent practices. With its principle-based guidance note, the CBB highlights its priorities in strengthening the cybersecurity posture of Belizean financial institutions. The principles are an appropriate interpretation of international best practices on incident prevention, detection, response, and recovery measures, adapted to the cyber maturity of the Belizean financial institutions, and can be used as a foundation for the formalized guidelines. The manual could emphasize the review of cybersecurity strategies, policies, and responsibility specifications and should address obtaining assurance on the effectiveness of the financial institutions' processes for cyber risk identification, assessment, and mitigation.

The CBB established a framework for timely cyber threat intelligence sharing between the financial institutions, however CBB's participation could be reconsidered because explicit participation of the supervision staff[2] may adversely impact timely information sharing. Representatives from the CBB, domestic and international banks, meet regularly in the cyber security committee (CSC) for financial services. The CSC provides a forum for strategic and tactical discussions on both evolutions in the cyber threat landscape and the cybersecurity innovations. Experience suggests that institutions may be wary sharing information on incidents and vulnerabilities when supervisors participate in such frameworks. It is thus preferable that CBB is represented by IT staff having no supervisory roles.

Currently IT inspections are conducted by technical experts from the IT department, which may put a strain on resources and pose a conflict of interest risk with the CBB's payment systems oversight role;[3] therefore, a dedicated IT supervision team should be established. International best practice is to ensure that supervisory and oversight activities are separated from the central bank's IT operations. A clear separation between the two functions significantly increases the independence and credibility of the oversight of the CBB operated financial services like the automated payment and securities settlement system (APSSS).

Disaster recovery at the CBB is facilitated by a partially redundant infrastructure, a robust replication and backup system, a comprehensive set of documented recovery

[2] Or technical experts from the IT department performing supervisory roles.

[3] The conflict of interest stems from the fact that the IT department runs the APSSS payments system and at the same time it is supposed to provide expertise for the oversight function.

procedures, and regular tests. Overall, these elements of the BCM framework provide for reliable and timely recovery of critical IT systems.

Key components of the IT infrastructure are redundant. These include critical servers (TechOne, APSSS, and Society for Worldwide Interbank Financial Telecommunication [SWIFT]), core network switches, firewalls, and the Wide Area Network (WAN) link to the disaster recovery (DR) site in Belmopan. Thus, as far as critical IT services are considered, single points of failure are largely eliminated.

While DR measures that address equipment and the building are generally adequate, business continuity measures that address alternate ways to run the business processes are lacking. Most notably, there are no contingency plans for alternate work arrangements and there is no standby office space available in case the main building becomes inaccessible.

The mission recommends four key steps to improve cybersecurity regulation and supervision. These are: (i) issue enforceable cybersecurity guidelines; (ii) develop a supervisory manual aligned with the supervisory guidelines; (iii) set up a dedicated IT supervisory team composed of at least two inspectors; and (iv) develop a rulebook for operational threat intelligence sharing between technical experts in the CSC.

The mission recommends six key steps to improve the BCM of the CBB. These are: (i) enhance the BCM framework with several measures (detailed in the report); (ii) designate a business continuity planning (BCP) project sponsor with sufficient authority to drive the cross-departmental work that is needed; (iii) in the BCP project focus on alternative operations and standby facilities; (iv) have all organizational units participate in the BCP project (their main responsibilities being detailed in the report); (v) specialized BCP software may be used but its benefits are unlikely to be fully realized; and (vi) consider external support for the BCP project;

The mission recommends three key steps to improve the cybersecurity governance of the CBB. These are: (i) consider the establishment of a cybersecurity function independent from IT; (ii) implement a formal cyber risk assessment process; and (iii) ensure staff responsible for the risk assessment receives relevant training. These steps with their priority and timeline are summarized in Table 1.

Table 1. Key Recommendations

Recommendation	Priority	Timeframe[4]	Reference
Cybersecurity Regulation and Supervision			
Issue enforceable cybersecurity guidelines.	High	Short-term	9.
Develop a supervisory manual aligned with the supervisory guidelines.	High	Short-term	10.
Set up a dedicated IT supervisory team composed of at least two experts.	High	Short-term	29.
Develop a rulebook for operational threat intelligence sharing between technical experts in the Cyber Security Committee.	Medium	Short-term	20
BCM			
The BCM framework should be enhanced with several measures (detailed in the report).	High	Short-term	52
The Board should designate a BCP project sponsor with sufficient authority to drive the cross-departmental work that is needed.	High	Short-term	53
The BCP project should focus on alternative operations and standby facilities.	High	Short-term	54
All organizational units should participate in the BCP project (their main responsibilities being detailed in the report).	High	Short-term	55
The plans should be regularly tested, and the test results should be used to improve them.	High	Short-term	58
External support for the BCP project should be considered.	Medium	Short-term	57
Cybersecurity Governance			
Consider the establishment of a cybersecurity function independent from IT.	High	Short-term	60
Implement a formal cyber risk assessment process.	High	Shot-term	61
Ensure staff responsible for the risk assessment receives relevant training.	High	Short-term	62.

[4] Short-term: < 12 months; Medium-term: 12–24 months.

I. Introduction

1. **The mission focused on two topics: (i) the Belizean regulatory framework for cybersecurity and the CBB's IT supervisory practices, and (ii) the cybersecurity resilience and governance elements of the CBB's internal BCM framework**. To achieve its goals, the mission reviewed relevant documentation, such as the cybersecurity guidance note, the terms of reference of the CSC, sample reports, plans, policies, procedures, risk assessments, and other internal IT and information security documents. The mission team interviewed senior staff to understand the context of the regulation, supervisory practices, cybersecurity governance, and BCM practices. The mission team also reviewed the physical and environmental control environment of the data center. Discussions were held on key cybersecurity topics, such as risk assessments, organizational structures, allocation of responsibilities to organizational units, effective practices, and tools. Finally, the mission held a BCM workshop for the CBB's management and met with industry representatives to present and discuss trends in regulation and supervision.

2. **This report is divided in five sections.** Section II addresses the current cybersecurity regulation in the Belizean financial sector, Section III outlines the cybersecurity supervisory practices, Section IV addresses cyber resilience at the CBB with focus on BCM, and Section V describes the suggested next steps.

II. Cybersecurity Regulation

A. Assessment

3. **Cybersecurity supervisory expectations are presented in an informational principle-based guidance note.** The guidance note on cybersecurity for the financial sector of Belize highlights the priorities of the central bank with respect to critical asset and risk identification processes. Specific requirements regarding incident prevention, detection, response, and recovery measures—aligned with international standards like the National Institute of Standards and Technology (NIST) Cyber Security Framework—are specified in the note. Furthermore, the note stresses the responsibility of both the institutions' board members and senior managers and recommends the establishment of a chief information security officer position. With this note the CBB aims to strengthen the cyber resilience of the Belizean financial institutions.

4. **The CBB has adequate regulatory and supervisory powers to promote cybersecurity in the Belizean financial sector.** The CBB can promulgate both mandatory rules and guidance and has sufficient legal authority to take enforcement action on any cybersecurity shortcoming at institutions within its remit, including the issuance of directives to rectify noncompliance and fines.

5. **A CSC for the financial services industry has been established.** Its roles are to (i) share information about the evolving cyber threat landscape; (ii) discuss cybersecurity

baselines and innovations; and (iii) timely communicate actionable information on cyber threats and incidents. The CSC is a national industry group in which the CBB, domestic, and international banks are represented by their senior officials with responsibilities related to cybersecurity. A CSC session on the current evolutions in the threat landscape, the need for adequate cybersecurity measures and resilience planning was hosted in the context of the mission.

6. **The presence of the supervisory authority in the CSC may limit cyber threat intelligence sharing by its members.** Trust relationships between industry participants typically form the basis for information sharing and collaboration during major cyber incidents. Participation of the supervisors in the CSC may result in a perceived threat of (immediate) supervisory action upon disclosure of incident information, which may adversely impact timely information sharing.

7. **The CBB is a member of the National Task Force for Cybersecurity.** Currently the task force develops the National Cybersecurity Policy and contemplates the establishment of national and sectoral computer emergency response teams. In addition to its legal prerogatives, this role has the potential to strengthen the CBB's credibility and soft power in cybersecurity supervision.

8. **Cybersecurity incident reporting is standardized with a reporting template**. The cybersecurity incident reporting template adequately covers the different elements of the incident, in other words, the occurrence and detection time of the incident, the attack vectors deployed by the cyber attackers, the classification and the impact assessment. Furthermore, it probes into the identified indicators of compromise and the response steps—containment, eradication, and recovery—taken by the affected financial institution.

B. Recommendations

9. **The CBB should issue formal guidelines on cybersecurity, which consider the status and cyber risk exposure of the Belizean financial institutions.** A hierarchical approach of stable principle-based regulatory objectives with more concrete supervisory interpretations is advised. Supervisory interpretations can more flexibly evolve with emerging cyber threats. Additionally, this approach allows for the introduction of proportionality in cybersecurity requirements, as influenced by the size and systemic importance of financial institutions, by adapting the control maturity expectations and not the control coverage. For example, identity management is a key control requirement applicable to all financial sector participants but the way it is implemented can vary from simple manual methods in case of a small institutions to sophisticated automated solutions in case of large or systemic institutions.

10. **The Supervision Department should take ownership of the formal requirements and maintain the evolving supervisory expectations for cybersecurity.**[5] The current guidance note focuses on those areas that the CBB deems most pertinent at this time. However, the regulatory requirements should be (i) extended to cover all areas of cybersecurity as outlined in international standards and (ii) strengthened to provide an adequate minimum cybersecurity baseline in face of the increasing risk of cyber incidents.

11. **The cybersecurity principles should be based on internationally accepted standards and good practices outlined in regulation from other jurisdictions.** For example, at a high level, the Group of Seven Fundamental Elements of Cybersecurity for the Financial Sector could be a starting point. This framework is succinct, easy to understand to non-technical audiences, and easy to map to more detailed frameworks, such as the NIST Cybersecurity Framework, the International Organization for Standardization 27000 series, or the Control Objectives for IT (COBIT). These frameworks could be referenced as examples of technically oriented tools that provide details beyond the regulation. The regulation should not prefer or require any specific framework nor specific technology. Based on the discussions the mission facilitated, country examples that could be considered include Canada, Australia, Singapore, or Kenya. Supporting tools, such as the Federal Financial Institutions Examination Council Cybersecurity Assessment Tool or the Office of the Superintendent of Financial Institutions (OSFI) Cyber Security Self-Assessment Guidance could provide valuable input to the development of the cybersecurity principles and supervisory interpretations.[6]

12. **The principles should emphasize the continuous improvement approach to cyber risk management and the pivotal role of the risk and control assessment in it.** The continuous improvement cycle concept is widely used in cyber risk management systems and it hinges on a realistic and comprehensive risk assessment. The principles and supervisory interpretations should promote minimum scope, timing and follow-up requirements for the risk assessment. However, it should remain agnostic on the risk assessment methodology, which should be assessed in the supervisory process. Consideration should be given to requiring the institutions to inform the supervisor on the outcome of their risk and control assessment. Falling behind deadlines with its execution and the consequent action plan could form the basis of supervisory action.

13. **The principles should require that risk and control assessments are based on comprehensive information asset identification and classification.** Information asset

[5] The current guidance note was developed by the IT department because the absence of cybersecurity skills in the supervision department.

[6] Jurisdictions and tools are mentioned as examples and should not be taken as preferences of the mission or IMF in general. A useful resource for many regulatory frameworks worldwide is the FSB Stocktake of Publicly Released Cybersecurity Regulations, Guidance and Supervisory Practices, which can be accessed at http://www.fsb.org/wp-content/uploads/P131017-2.pdf.

classifications should be based on the three fundamental security objectives, in other words, preserving the confidentiality, integrity, and availability of information assets. Institutions should be free to choose their own classification scheme, provided that critical assets are clearly identified.

14. **Cyber risk management responsibilities for the board and senior management of the financial institutions should be clearly specified in the guidelines.** This will generate incentives to significantly improve the cybersecurity posture. While the board and senior management are ultimately responsible for respectively approving and implementing the financial institution's cybersecurity strategy, they typically underappreciate the business implications of cyber risks. As a result, the board and senior managers are inclined to subordinate cyber resilience to other business objectives. Specific cybersecurity guidelines create visibility for cyber risk to the members of the board and senior management.

15. **Special provisions for material outsourcing arrangements should be considered, including notifications, formal rights to audit, and incident reporting requirements.** Financial institutions should be required to maintain a comprehensive register on their outsourcing arrangements according to a predefined template. Requiring timely notification on material outsourcing and an annual reporting of the outsourcing registers supports the supervisors in their own cyber risk assessment and supervision planning processes. An explicit definition of material outsourcing by the CBB in line with international standards would ensure reporting consistency and make the supervisory process more effective. Outsourcing agreements should explicitly require service providers to accommodate audits from the institutions and the CBB, as well as reporting requirements for relevant cyber incidents.

16. **Incident reporting requirements should specify a comprehensive classification scheme for cyber incidents and materiality thresholds.** To make incident reporting information more actionable, the CBB should consider outlining criteria and specifying related thresholds to determine whether an incident is of sufficient magnitude to be reportable and within which timeframe. These criteria could include the criticality of affected systems, value, and number of transactions involved, downtimes, economic/reputational impact and incident category.

17. **The principles should require regular control implementation effectiveness assessments like penetration testing as an important risk management activity for financial institutions.** Weaknesses in the configuration or source code of information systems and networks can be identified using vulnerability scanners. Penetration testing is a more sophisticated approach in which ethical hackers simulate complex attack vectors to identify areas where the financial institutions are the most vulnerable. Furthermore, penetration testing makes it possible to assess the maturity of the institutions' cyber incident detection, and response capabilities. Leading jurisdictions require the ethical hackers to base

their attack vectors on advanced cyber threat intelligence, which considers the tactics, techniques, and procedures of the institutions' expected cyber adversaries.

18. **The principles should give due attention to scenario-based cyber resilience planning and exercising.** Cybersecurity incidents with a significant impact on the confidentiality, integrity, and availability of critical assets are increasingly common. Financial institutions could improve their cyber resilience by proactively developing cyber incident management plans. Important during the development of these incident response plans is recognizing the multiple facets of dealing with cyber incidents; for example, impact on business operations, legal requirements, communication to stakeholders, and human resources. Recently observed attack vectors like those of crypto-ransomware or fraudulent wholesale payments, form a good basis for scenario-driven testing of the incident response plans.

19. **Additional key areas to be covered by the principles are (i) governance, (ii) strategy, (iii) monitoring and detection, (iv) response, (v) recovery, and (vi) information sharing.** The principles should address cyber governance with a focus on establishing, implementing and reviewing cyber risk management processes. Internal control specifications in the cybersecurity principles, and supervisory interpretations should focus on preventing the materialization of cyber risks and on enabling containment of cyber incidents (e.g., network segmentation). Also, the guidelines should require financial institutions to develop effective detection, response, and recovery capabilities.

20. **Effective sharing of operational threat intelligence like indicators of compromise, requires trust relations between technical experts of financial institutions and a rulebook.** The current membership of the CSC is well suited for strategic and tactical discussions on cyber threats, in other words, respectively information on evolutions in the threat actors and their motives and information on the trends in the actors' tactics, techniques, and procedures. Operational intelligence, like indicators of compromise and malicious IP-ranges, should be shared between information assurance and system/network operation professionals from the financial institutions, as well as members of national computer emergency response teams (currently being established). Information handling procedures such as traffic light protocols should be agreed upon. Special platforms exist for information sharing between central banks, regulators, and supervisory entities (e.g., Financial Services Information Sharing and Analysis Center, Central Banks, Regulators, and Supervisory Entities) in which the CBB could participate.

III. Cybersecurity Supervisory Practices

A. Assessment

21. **The CBB has adopted a general supervisory framework and methodology, which is grounded on international best practices and could be applied for IT supervision.** Onsite examination planning includes the identification of the IT expertise needed and

preliminary information gathering activities. IT related inspections are primarily based on interviews and walkthroughs, which may include on the spot correction of identified issues. The CBB formally follows up the supervisory findings.

22. **Supervisory reporting is exception-based.** Institutions have the opportunity to comment on the factual correctness of the findings before the report is issued**.** The supervisors record a description of the existing control framework within scope and concisely describe their supervisory findings during the inspection. After the factual correctness discussion with the supervisees, the supervisor develops a report that details the open supervisory findings[7] with recommendations and deadlines. Currently supervisors do not rate their findings.

23. **The supervisory IT examinations are conducted in collaboration with experts from the IT Department.** Expertise in information systems governance, processes, and technology is currently very limited within the supervision department. The reliance on internal experts may put a strain on resources of the IT department and pose a conflict of interest risk with the CBB's payment systems oversight role. The conflict of interest risk arises because the IT department is in charge for operating and supporting the payment system infrastructure, including its cybersecurity controls, so they cannot be reasonably expected to perform oversight duties in an independent way. The CBB has started the hiring process for a dedicated IT supervisor.

B. Recommendations

24. **A supervisory manual for IT/cybersecurity inspections aligned with the cybersecurity guidelines and supervisory expectations should be developed**. Determining whether the management of the financial institutions actively promote effective cybersecurity governance has been identified as a key supervisory priority. To this end, the manual could emphasize the review of cybersecurity strategies, policies, and responsibility specifications. Additionally, the manual should address obtaining assurance on the effectiveness of the financial institutions' processes for cyber risk identification, assessment, and mitigation. These assurance activities should be supplemented with a review of the cyber risk reporting processes and an analysis of the effectiveness of the oversight by independent functions like the board of directors, the internal audit department, and external auditors. Furthermore, the manual should include procedure probing into resourcing of the relevant cybersecurity functions and third-party service provider management. Finally, the manual should provide guidance on evaluating the provisions for cyber incident response and resilience.

25. **Supervisory risk assessments should consider technical assessments by credible third-party assurance providers and the financial institutions' internal audit.**

[7] Where possible, the supervisors allow for on-the-spot correction of findings. Open supervisory findings are defined as the issues that require more complex corrective actions.

Independent opinions on relevant cybersecurity measures could be found in internal and external audit reports, independent security tests like penetration testing reports and service provider mandated endpoint security assessments like SWIFT Customer Security Program self-assessments (preferably backed by independent assurance). Furthermore, reviewing the management's responses to issues raised in the previously mentioned reports could provide important insights; for example, willingness to remediate shortcomings in IT governance, infrastructure, applications, and processes. The reliance on internal audit reports should be informed by the supervisor's rating of the internal audit function in terms of quality and independence.

26. **Self-assessments by the financial institutions could provide the supervisor with significant input for their risk assessment and assist in scoping offsite and onsite inspections.** The cybersecurity self-assessment typically forms an integral part of the pre-examination information request, which may highlight both limitations in the control framework and important changes to the IT environment of a financial institution. Areas that could be addressed in the cybersecurity self-assessment include: (i) cybersecurity governance and strategy; (ii) presence of critical cybersecurity control measures for prevention and detection of cyber incidents, including the establishment relevant policies; (iii) processes for cyber risk identification and assessment; (iv) control effectiveness assessments recently conducted; (v) situational awareness in terms of critical assets and evolutions in the cyber threat landscape, such as up to date risk assessments; (vi) third-party risk management; and (vii) cybersecurity incident management. Some supervisory authorities request the supervisees to indicate the maturity level with which a certain cybersecurity area has been met and to provide supporting evidence (e.g., policy documents and test reports). The cybersecurity self-assessment guidance from the Canadian OSFI was identified as an interesting starting point.

27. **The CBB should consider including evidence supporting the findings in the examination reports.** Currently, supporting evidence is used in the discussions with the institutions prior to the compilation of the report. However, including such evidence in the report provides a strong ex post justification for the recommendations in one official document and avoids any ambiguity later on. Alternatively, the supervisor may opt for references to supporting evidence included in the work papers, which allows for a better tracking. The CBB may also consider the adoption of a rating scheme for findings, which reinforces the need to timely close significant issues.

28. **More emphasis should be placed on onsite control effectiveness examination procedures.** Offsite analysis of policy documents and control descriptions provide insights in the control design and enables the supervisors to assess the design adequacy. Onsite cyber control effectiveness examination procedures, on the other hand, give a firsthand look at what is going on in the financial institutions under supervision. As a result, these practices provide the supervisor with a better understanding of control implementation effectiveness.

29. **The CBB should decrease the reliance on internal IT staff in the supervisory process and establish a dedicated IT supervision team composed of at least two inspectors with adequate expertise and qualifications.** International best practice is to ensure that supervisory and payment systems oversight activities are separated from the central bank's IT operations. A clear separation between the two functions significantly increases the independence and credibility of the oversight of the CBB operated financial services like the APSSS payment system. Internationally recognized certifications like ISACA's certified information systems auditor (CISA) and (ISC)² Certified Information Systems Security Professional (CISSP) provide adequate background for IT supervisory activities. There exists a global strain on professionals with the expertise required for IT supervision. Recent research has indicated that the three most effective incentives to attract and retain cybersecurity experts are: (i) offering significant training opportunities (including paying for security certification); (ii) improving compensation packages; and (iii) flexible work schedules. Additionally, the CBB should consider potential process efficiency gains like relying on the internal audit function of the financial institutions to follow-up and report on the resolution of findings, provided that the function's quality and independence is deemed to be adequate.

30. **When planning the supervisory calendar for the coming year, capacity should be allocated to ad-hoc examinations due to unforeseen circumstances.** The revisiting interval of one and a half year as specified in the CBB's internal supervisory objectives is considered acceptable. Introducing more differentiated intervals based on systemic importance and cybersecurity risk posture could be considered, however. Spare capacity should be foreseen to deal with incidents and provide an effective and timely supervisory response.

IV. Cyber Resilience

A. Assessment

31. **The mission focused on the BCM aspect of cyber resilience at the CBB and addressed cybersecurity governance as well.** Operational cybersecurity, while some topics were discussed, was not addressed in an exhaustive manner and is not covered in this report.

– BCM

32. **DR at the CBB is facilitated by a partially redundant infrastructure, a robust replication and backup system, a comprehensive set of documented recovery procedures, and regular tests.** Overall, these elements of the BCM framework provide for reliable and timely recovery of critical IT systems.

33. **Key components of the IT infrastructure are redundant.** These include critical servers (TechOne, APSSS, and SWIFT), core network switches, firewalls, and the WAN link to the DR site in Belmopan. Thus, as far as critical IT services are considered, single points of failure are largely eliminated.

34. **However, it is unclear what is the redundancy of the WAN link to the DR site.** There is no definitive information at the CBB whether this multiprotocol label switching service provided by a local telecommunications company is physically redundant between the main and DR sites or not.

35. **The data center power supply is very resilient against outages.** There is an uninterruptible power supply system capable of delivering enough power to the data center for 45 minutes, and two power generators at the opposite ends of the building with one month's worth of fuel reserves. The generators can be activated within minutes and are regularly tested and maintained.

36. **The physical protection of the main data center is lacking.** A large portion of an internally facing wall is of glass, which leaves critical IT equipment rather vulnerable to physical damage. Fire suppression is inadequate, with only one handheld extinguisher. Additionally, the large glass surface does not sufficiently shield electromagnetic radiation. This, given the exposed location, makes wireless exfiltration attacks more feasible.[8]

37. **Critical systems' data are replicated to the DR site in Belmopan in real time, which minimizes the risk of data loss.** Replication is set up for all important virtual machines as well, with appropriate recovery point objective (RPOs). As a result, the resilience to disruption of critical and important IT services is good.

38. **Non-critical systems are backed up to tapes according to a predefined schedule.** The tape technology is relatively old but very reliable if the tape cartridges are used within specifications. However, the old tape system is being phased out and there is a project underway to do data backup consolidation.

39. **The CBB does regular recovery tests for the critical systems.** Results indicate a high degree of resilience of the APSSS, TechOne and SWIFT systems. Processing can be switched over to the DR site within minutes without data loss. However, this is dependent on the availability of the WAN link. Recovery tests for other systems are performed from time to time as well, but only the critical systems receive constant attention in this regard.

40. **The CBB has an up to date hurricane plan that is tested each year before the hurricane season.** Shortcomings identified during the tests are addressed in a timely manner.

41. **The CBB is in the process of upgrading the physical security management system (SMS).** The system is going to support strong user authentication using smart card technology. SMS servers will run on a segregated network infrastructure and will be

[8] For example, a rogue access point's signal could be picked up from outside of the building.

accessible from the office network through a dedicated firewall. Also, the security control room is being retrofitted for the SMS system.

42. **The CBB main building is designed to withstand major hurricanes and storm surges of up to 15 feet.** This level of resilience is considered adequate despite the building's coastal location.

43. **While disaster recovery measures that address equipment and the building are generally adequate, business continuity measures that address alternate ways to run the business processes are lacking.** Most notably, there are no contingency plans for alternate work arrangements and there is no stand-by office space available in case the main building becomes inaccessible.

– Cybersecurity Governance

44. **Cybersecurity responsibilities are assigned to the IT Department.** There is a security analyst who reports to the manager of the IT department. Other staff also perform security related activities as needed. Because the IT department is small, this model is efficient. The only other unit that has some degree of cybersecurity capacity is internal audit, where one staff is training to become a CISA.

45. **The manager of the IT department reports to the senior manager of corporate services, who in turn reports to the governor.** This is considered an adequate reporting line for IT at the CBB, given the small size and relatively simple organizational structure.

46. **An enterprise risk management (ERM) function has been recently established.** The CBB has a variety of different departments and functions each managing specific risks, for example, IT security or succession planning for key personnel. With the establishment of an ERM function, the CBB aims at coordinating between the different functions and creating an integrated risk management framework. Currently, there is only one relatively junior staff dedicated to ERM and she has no cybersecurity expertise.

47. **The inclusion of all cybersecurity related responsibilities in the IT Department, in combination with little relevant expertise available in ERM and internal independent assurance functions increase conflict of interest risk.** The internal audit department and the external auditor do not provide adequate compensating controls at this time.

48. **There is a very well structured and developed IT policy framework that addresses many cybersecurity areas as well.** The IT department strives to maintain all policies and procedures and while some lag can be observed, key policies and procedures are up to date and actionable.

49. **The IT risk assessment done by the IT department[9] is a good start, however improvements are necessary.** The risks identified are relevant in general, but not sufficiently specific to the CBB. Risk ratings based on impact and likelihood assessments are missing. The controls listed are more specific (for example they reference actual procedures) but their effectiveness is not assessed, and residual risks are not determined. Therefore, it is unclear which areas need additional or strengthened controls. It follows that remedial action cannot be defined and indeed it is missing. Further, there is no evidence of risk acceptance and senior management signoff. The root cause of these deficiencies appears to be the lack of formalized and methodology-based risk assessment expertise in the IT department.

50. **Penetration testing by third parties provide a degree of independent assurance over the effectiveness of the cybersecurity control environment.** The IT department remediates the findings of the tests.

51. **Incident management is not sufficiently formalized.** The IT department has developed a draft incident response plan based on the NIST Computer Security Incident Handling Guide. While the plan requires the cooperation of other organizational units, there is no evidence on their involvement in the development of the plan nor on their acceptance thereof.

B. Recommendations

– BCM

52. **The BCM framework should be enhanced with several measures.** These are: (i) initiating a BCP project; (ii) assigning BCM responsibilities to all organizational units for the processes and resources they are responsible of; (iii) providing sustained senior management support; and (iv) improving the physical protection of the data center.

53. **The Board should designate a BCP project sponsor with sufficient authority to drive the cross-departmental work that is needed.** Typically, this responsibility is often assigned to a senior executive role, such as the chief operations officer or a similar. The project sponsor should have a good understanding of the CBB's operations and its operational risk profile.

54. **The BCP project should focus on alternative operations and standby facilities.** At the same time, existing IT disaster recovery action plans (procedures) should be reviewed and updated as necessary. If the business impact analysis (BIA) phase of the project identifies resources lacking a recovery action plan those should be developed as well. As part

[9] Referred to as the IT Table of IT Risks.

of the project, attention should be paid to developing a BCM policy that addresses training, testing and maintenance of the plan, among others.

55. **All organizational units should participate in the BCP project, their main responsibilities being as follows:** (i) input to the BIA, such as identification and prioritization of processes and resources, setting recovery time objectives, and RPOs; (ii) building action plans for alternate operations; and (iii) participation in training, testing, and maintenance according to the BCM policy.

56. **While a specialized BCP software could be helpful, given the small size of the CBB it is unlikely that its benefits would be fully realized.** Standardized templates developed with office applications can work well without any additional licensing costs. The downside of the approach is more manual work and the lack of an automatically enforced methodology.

57. **External support for the BCP project should be considered.** Experienced BCP professionals can add value by bringing in a proven methodology**,** templates, techniques and practices that help avoiding common pitfalls and shorten the duration of the project.

58. **The plans should be regularly tested, and the test results should be used to improve them.** Tests should range from simple table-top exercises to more complex simulations and should be based on scenarios as realistic as possible. After gaining experience, disruptive tests could be considered as well, whereby the data center is shut down and processing and key staff is transferred to disaster recovery locations. Such tests require extensive preparation and planning and are typically done less frequently.

59. **Assurance over the redundancy of the WAN link to the DR site should be obtained.** This could be done by analyzing information from the telecommunications provider, including network architecture, equipment and line redundancy, and DR plans.

- **Cybersecurity Governance**

60. **Consideration should be given to the establishment of a cybersecurity function independent from IT.** The main responsibility of such a function would be to develop and maintain the cybersecurity governance framework and to control cybersecurity processes and systems. This change has several advantages: (i) it implements an independent control layer over security critical IT activities; (ii) in the longer term it can concentrate scarce cybersecurity expertise which helps attaining critical mass needed for an effective cybersecurity function; and (iii) it reduces the IT department's workload. In addition, this allocation of responsibilities is more closely aligned with how cybersecurity units operate at other central banks and many commercial banks. Examples of processes and systems that could be controlled by the independent cybersecurity functions include identity and access management, perimeter defense, endpoint protection and anti-malware, web content filtering, data loss protection, and security information and event management. In this context, transfer

of control from IT does not necessarily encompass transfer of ownership of the underlying infrastructure. Rather, the cybersecurity unit could act as a control point, for example, it approves firewall rules but does not run the firewall itself. Other areas where the independent cybersecurity control is beneficial are IT architecture, system implementation projects, and use of third parties. For example, the unit's signoff should be required on changes to the network architecture, on procuring or developing new systems, or on using cloud services. Given the CBB's organizational structure, best options for the reporting line for the cybersecurity functions include the governor, corporate services, and security. Each option has advantages and disadvantages. Reporting to the governor would increase visibility but distances the function from IT; reporting to security would consolidate all security related functions but has the same disadvantage. Reporting to corporate services is probably the most balanced option because of the appropriate level in the hierarchy and closeness to the IT department.

61. **A formal cyber risk assessment process should be implemented.** The process should: (i) consistently apply a documented risk assessment methodology (usually qualitative); (ii) define the risk appetite, for example, by setting the maximum level of acceptable residual risk; (iii) require risk mitigation measures for all residual risks above the appetite; (iv) ensure the involvement of the business units especially in risk identification and rating; (v) require the risk mitigation measures to be documented in an action plan with deadlines and clearly identified responsibilities; (vi) ensure the action plan gets appropriate funding; (vii) ensure timely follow-up on the action plan; and (viii) ensure regular updates and Board reporting.

62. **Staff responsible for the risk assessment should receive relevant training.** Several development tracks for improving cybersecurity risk assessment skills could be considered, including (i) a series of courses like the ones provided by SANS Institute targeting both generalists (e.g., A Practical Introduction to Cyber Security Risk Management—MGT415) and IT experts; (ii) review of international standards such as ISACA's COBIT and Committee of Sponsoring Organizations of the Treadway Commission's ERM framework; or (iii) training for the CISSP or Certified Information Security Manager certifications.

63. **The incident management plan should be circulated to involved business units, their feedback addressed, and the updated plan formally approved.** Agreeing upon specific escalation criteria, processes and contacts forms an integral part of an effective incident management plan.

V. NEXT STEPS

64. **The CBB should develop an improvement plan to address the findings.**