INTERNATIONAL MONETARY FUND

IMF Country Report No. 23/161

TRINIDAD AND TOBAGO

TECHNICAL ASSISTANCE REPORT-STRENGTHENING CYBERSECURITY IN FINANCIAL INSTITUTIONS

May 2023

This Technical Assistance Report on Trinidad and Tobago was prepared by a staff team of the International Monetary Fund. It is based on the information available at the time it was completed in February 2023.

Copies of this report are available to the public from

International Monetary Fund • Publication Services
PO Box 92780 • Washington, D.C. 20090
Telephone: (202) 623-7430 • Fax: (202) 623-7201
E-mail: publications@imf.org Web: http://www.imf.org
Price: $18.00 per printed copy

International Monetary Fund
Washington, D.C.

TECHNICAL ASSISTANCE REPORT

TRINIDAD AND TOBAGO

STRENGTHENING CYBERSECURITY IN FINANCIAL INSTITUTIONS

February 2023

Prepared By

Rangachary Ravikumar
Tamas Gaidosch

Authoring Departments:

Monetary and Capital Markets Department

Contents **Page**

GLOSSARY

Acronym	Details
ACH	Automated Clearing House
BCP	Business Continuity Plan
CBTT	Central Bank of Trinidad and Tobago
CSP	Customer Security Program
DR	Disaster Recovery
FFIEC	Federal Financial Institutions Examination Council
FISD	Financial Institutions Supervision Department
FIUTT	Financial Intelligence Unit of Trinidad and Tobago
FTE	Full Time Equivalent
IAM	Identity and Access Management
ICAAP	Internal Capital Adequacy Assessment Process
ICT	Information and Communication Technology
IT	Information Technology
MCM	Monetary and Capital Markets Department
MYND-CDD	Ministry of Youth and National Development - Cooperative Development Division
RBS	Risk Based Supervision
RFI	Request for Information
RFP	Request for Proposal
TTSEC	Trinidad and Tobago Securities and Exchange Commission
TA	Technical Assistance

PREFACE

At the request of the Central Bank of Trinidad and Tobago (CBTT), the Monetary and Capital Markets Department (MCM) provided a field based technical assistance (TA) mission on strengthening cybersecurity in financial institutions during October 31 to November 4, 2022.

The purpose of the mission was to (i) strengthen the cybersecurity of the financial institutions under the supervisory ambit of CBTT and build supervisory capacity for the effective supervision of cybersecurity and (ii) strengthen the cybersecurity posture of the Central Bank.

The mission had met the Governor on the first day. The mission met Patrick Solomon (Inspector), Michelle Francis-Pantor (Deputy Inspector) from Financial Institutions Supervision Department (FISD) and Frances Correa (IT Consultant) and their team members.

This report presents the mission's assessment and main conclusions. The mission wishes to thank the officials of the CBTT for their excellent cooperation and productive discussions.

EXECUTIVE SUMMARY

At the request of the CBTT, a TA mission on strengthening cybersecurity in financial institutions was delivered during the period October 31–November 4, 2022. The Governor requested the TA during the 2022 Spring Meetings and the deliverables for the mission and the milestones were identified by having a dialogue with the authority. The mission had two objectives: (i) to strengthen the cybersecurity of the financial institutions under the supervisory ambit of CBTT and (ii) to improve the cybersecurity stance of the CBTT. For the project for strengthening cybersecurity of the Central Bank an internal project team has been constituted. For strengthening cybersecurity of financial institutions, the CBTT has established a working group comprising all the financial regulators (namely, the CBTT, Trinidad and Tobago Securities and Exchange Commission (TTSEC), the Financial Intelligence Unit of Trinidad and Tobago (FIUTT), and the Office of the Commission of Cooperative Development (CCD) to draft a cybersecurity guideline for financial institutions and a supervisory manual.

The deliverables included a capacity building seminar on regulation of cyber risk. The seminar was delivered during November 1–3, 2022 covering cyber threat landscape, cyber risk and financial stability, impact of new technologies on cyber risk, international regulatory practices, cyber risk governance and management best practices, third party risk management, incident reporting, business continuity planning, response and recovery, information sharing, and testing. The seminar was attended in person and remotely by supervisory officials from all the regulatory authorities, although at this time, the CBTT is the only regulator that intends to draft a guideline on the subject.

The CBTT identified the need for filling regulatory gaps and desires to issue a focused guideline on cybersecurity covering governance, risk management, incident reporting, and cyber hygiene, and intends to develop a draft guideline for consultation with its regulated institutions in the first quarter of 2023. Currently, there are no Information and Communication Technology (ICT) or Cyber risk guidelines issued by the CBTT. These aspects are governed indirectly by the extant instructions on corporate governance, market conduct, security systems for safeguarding customer information, Internal Capital Adequacy Assessment Process (ICAAP), and outsourcing. Discussions with a couple of banks indicate that the regulated entities may perceive it differently and do not consider these instructions to be directly applicable to ICT/cyber risk management underlining the need for a separate regulatory guidance. The mission had multiple rounds of discussion with the intra-agency working group constituted for the purpose of providing guidance in developing the guideline.

Supervisory arrangements for ICT/cyber risks need further improvements and resource constraints within FISD need to be addressed urgently. The organizational structure of the FISD indicates responsibilities for supervising banks and nonbanks was entrusted to one division and insurance and pension firms to another. There is no practice of assigning a dedicated supervisor even in the case of top five banks. Similar arrangements were there for insurance and pension firms. CBTT recognizes the importance of cyber risks and have taken some steps

including conducting thematic reviews of banks periodically on cyber related topics, carrying out cyber risk assessments for banks and sensitizing the financial sector participants on the need for enhanced cybersecurity. It is important to increase the frequency and intensity of ICT/cyber examinations particularly for large banks. This would require the resources to be augmented urgently. To date, insurance and pension firms have not been subjected to any survey on cyber related topics and regulatory/supervisory initiatives to address ICT/cyber risks are limited.

To help improve the cybersecurity posture of the CBTT, the mission performed a high-level assessment of the cybersecurity governance and the Identity and Access Management (IAM) project. Both assessments were based on reviewing the relevant organizational and project structures, policies and procedures, and interviews with selected members of CBTT management and staff.

Key findings of the cybersecurity governance assessment are as follows:

(i) Cybersecurity governance at CBTT is set up according to generally accepted practices in the financial sector, with some minor differences and resource constraints;
(ii) The information security function in the first line[1] is subordinated to the Head of IT, which calls for compensating controls;
(iii) Unusually, the second line of defense–risk management–has a formal responsibility in driving IT governance, a first-line role;
(iv) Cybersecurity policies and procedures cover most of the important topics and have been recently updated;
(v) Policies governing the cybersecurity of payment systems are uneven in terms of the technical controls required. The SWIFT cybersecurity control environment is more comprehensive due to the formalized requirements of the Customer Security Program (CSP); and
(vi) There is not a separate Cyber Risk Committee or similar at the Board level, but the existing IT Committee assumes this function.

The IAM project has been formally set up and is now in Phase 1, which is considered preparatory. The governance of the project, the high-level roadmap, and the deliverables for Phase 1 are generally in line with good practices. The mission drew the attention of the project team to some key tasks in the near future, including getting input from the business functions, to do a roles and access rights review, and to develop formal requirements, among others. A summary of the recommended actions is given in Appendix I.

[1] In terms of three lines model articulated by the Institute of Internal Auditors (IIA) (The IIA's Three Lines Model – published by IIA), First line roles: Provision of products/services to clients; managing risk. Second line roles: Expertise, support, monitoring and challenge on risk-related matters. Third line roles: Independent and objective assurance and advice on all matters related to the achievement of objectives.

TABLE 1. KEY RECOMMENDATIONS

Recommendation	Priority	Time frame*	Reference Paragraph
Organization and capacity			
Augment the resources in ICT/cyber risk supervision	High	Immediate	15
Cyber Risk Regulation			
Draft the guideline on ICT/cyber risk covering banks, insurance companies and pension firms on the basis of various inputs provided in the Seminar on Regulations, striking an appropriate balance between general principles and specific details having regard to the local environment and digital landscape	High	Near Term	16
Include a provision in the guideline to conduct an independent periodic assessment of cyber preparedness of banks, insurance companies and pension firms by qualified external professionals	Medium	Near Term	17
Incorporate a requirement for the Board to identify the regulatory gaps, draw an implementation plan with appropriate milestones and submit to the CBTT as part of the guideline	High	Near Term	18
Prepare a cyber incident reporting template and require supervised entities to report cyber incidents in keeping with the requirements as defined in the guideline or template.	High	Near Term	20
Sensitize the regulated entities on the need for strengthening cybersecurity through speeches, interviews, etc., and impress upon the need for a separate guideline, cyber incident reporting and information sharing among banks	High	Near Term	21
Cyber Risk Supervision			
Plan and conduct ICT/cyber preparedness surveys among insurance companies and pension firms	High	Medium Term	22
Increase the frequency and intensity of ICT/cyber risk assessments, to start with for major banks.	High	Medium Term	23
Plan and augment supervisory resources to ensure a self-sufficient supervision function covering banks, insurance companies and pension firms	High	Medium Term	24
Consider setting up an offsite supervision function for ICT/cyber risks	Medium	Medium Term	25

Recommendation	Priority	Timeframe	Reference Paragraph
Cybersecurity governance			
Assess the workload of the IT Security unit and increase resources as needed.	High	Medium term	32
Remove IT governance from the responsibilities of the risk function.	High	Near term	33
Establish regular cybersecurity meetings and reporting regime at the Board level with the participation of the Head of IT Security.	High	Near term	34
Develop a secure application development policy and security hardening baselines.	High	Near term	35
Develop a policy to bring the cybersecurity controls of the ACH and RTGS systems more in line with the SWIF CSP.	High	Near term	36
Regularly commission security reviews and tests of the payment systems.	High	Near term	37
Disaster recovery tests should include simulating a complete failure in the primary data center.	High	Medium term	38
Identity and Access Management (IAM) project			
Plan out Phase 2 of the IAM project and include requirements definition and roles and access rights review as key tasks, among others.	High	Near term	44
Analyze the projected workload and expertise vs internal resources and skills to determine the type and extent of third-party support needed.	High	Near term	45
Adopt a phased approach to IAM deployment.	High	Near term	46
Adopt good IAM implementation practices listed in the Appendix as deemed necessary.	Medium	Near term	47

* *Immediate: less than three months; Near term (NT):* 3–6 months*; Medium term (MT):*6–12 months*; Long term (LT):* more than 12 months.

I. Introduction

1. **The mission focused on (i) strengthening the cybersecurity in financial institutions by providing guidance to draft a regulatory guideline, and (ii) helping improve the cybersecurity stance of CBTT by assessing the cybersecurity governance and the IAM project**. The mission conducted a seminar on cybersecurity regulation to build capacity within CBTT to draft a regulatory guideline and by way of discussion with stakeholders and analyzing the information provided by the CBTT assessed the supervisory capacity. To assess the cybersecurity governance the mission reviewed CBTT's relevant organizational structure, policies, and procedures. The documentation used for this work included organizational charts and approved policies and procedures, risk assessments, and other internal information security documents. The mission interviewed senior staff to understand the current cybersecurity governance practices. The IAM project was assessed in similar approach, focusing on the project charter, project plan, and planned deliverables. Due to the limited time available the mission relied on the information and documents as provided and did not seek independent corroboration.

2. **This report is divided in five sections.** Section II addresses the seminar on cyber risk regulation; Section III covers the financial sector cybersecurity guideline development and assessment of supervisory capacity; Section IV outlines the results of the cybersecurity governance; and Section V addresses the IAM project.

II. Seminar on Cybersecurity Regulation

3. **Delivering a seminar on cybersecurity regulation was an important component of the mission.** One of the objectives of the mission was to strengthen the cybersecurity in financial institutions by assisting the authorities in drafting and issuing a regulatory guideline. To facilitate the drafting work CBTT has constituted a working group comprising all financial sector regulators. The CBTT will take the lead on drafting the proposed guideline with input from the other regulators and the guideline will be issued only to those entities regulated by CBTT at the present time. In building capacity among supervisory staff of CBTT and other regulators, a seminar was organized covering important topics. The seminar spanned three days with three sessions each day. The agenda is given in Annex I. The seminar was received well as reflected in the feedback.

4. **The first day of the seminar covered Cyber Risk and Financial Sector – An Introduction, Implications for Financial Stability, Cyber Security – An Overarching Framework, and Cyber Security and New Technologies including Cloud Regulation.** First day's session introduced the importance of managing cyber risk within the financial sector by discussing emerging cyber threat landscape, evolution of banking technology, pace of digitalization, increasing intensity of cyberattacks and the transmission channels through which cyber risk could pose financial stability concerns. Arrangements at various countries in managing cybersecurity with a few country examples was discussed to provide a context to the financial regulators. The risks arising out of adoption of newer technologies like Artificial

Intelligence/Machine Learning, Application Programming Interface, and Cloud Technologies were discussed with specific focus on building regulatory guideline on these emerging areas of interest.

5. **An overview of the International Guidance on Cyber Risk and Global Regulatory Practices and third-party risk management were covered during the second day.** International guidance on cyber risk and global regulatory practices were covered to provide an overview of such arrangement covering the work of standard setting bodies and major regulators. By way of example, the regulations issued by two jurisdictions were discussed. Subsequently governance and risk management aspects were covered in depth. Session on third-party risk management highlighted the increased use of third parties within the financial sector, growing dependencies, regulatory best practices, and supervisory focus in assessing such arrangements.

6. **Incident reporting, information sharing, business continuity and response and recovery capabilities were discussed on the third day.** The third day's session focused on cyber incident reporting by discussing the ongoing work by standard setting bodies in this area and highlighting the usefulness of collecting such information. The need for the financial institutions to share information among themselves voluntarily on threat intelligence and best practices observed in this regard were also discussed. With the focus of the standard setting bodies on delivering critical financial services through disruption, business continuity and response and recovery capabilities within the financial institutions assume importance. This topic was covered extensively during the seminar.

III. Financial Sector Cybersecurity Guideline Development and Assessment of Supervisory Capacity

A. Assessment

7. **CBTT does not currently have a cybersecurity guideline in place applicable to its supervised entities.** The Corporate Governance Guideline, Guideline for the Management of Outsourcing Risks, Guideline for the Security Systems for Safeguarding Customer Information, Market Conduct Guideline and ICAAP Guideline cover certain aspects of ICT or cyber risk management including (i) Board having special skills including information technology, (ii) risk management framework to include provisions to evaluate the risks and materiality of all existing and prospective outsourcing arrangements and the inherent risks associated with outsourcing which includes cyber risk, (iii) management to be responsible for developing and documenting an operating manual of the policies, procedures and processes of the institution's information security program, (iv) reporting of material incidents to the CBTT, and (v) need to conduct stress tests with severe cyberattack as one of the scenarios. The current regulatory guidelines on the subject are fragmented and do not comprehensively address the issues given the growing importance of cybersecurity.

8. **CBTT has identified the regulatory gap and has constituted a working group duly represented by all financial sector regulators to draft a guideline on the topic.** CBTT is responsible for supervising banks, non-banks, insurance companies, pension firms, bureaux de change, and payment systems. The Trinidad and Tobago Security and Exchange Commission (TTSEC) supervises the securities market and intermediaries, and the Cooperative Development Division within the Ministry of Youth and National Development is responsible for supervision of credit unions. The Financial Intelligence Unit has jurisdiction over Anti Money Laundering/Countering Financing of Terrorism cutting across various nonfinancial sectors. Only CBTT proposes to draft a guideline while other regulators felt lessons learnt in the drafting exercise would be beneficial to introduce a similar guideline at an appropriate time.

9. **Among the CBTT supervised entities, banks appear to be better informed on ICT/cyber risks compared to other entities like insurance and pension firms.** Banks' IT systems have been under the focus of FISD for some time now and some of the guidelines make it incumbent on banks to manage the IT risks. Periodic surveys carried out by the CBTT has also played a role in sensitizing them on this important topic. Risk-Based Supervision (RBS) Manual also covers assessment of IT risks as part of operational risk and provides some guidance to supervisors, though the Manual is outdated (version shared with the mission is dated 2003) and due for revision in 2023. Desk-based reviews through virtual engagement with banks also are good initiatives. FISD used current best practice frameworks (Federal Financial Institutions Examination Council's (FFIEC) cybersecurity assessment tool) in assessing the exposures of the banking sector to cyber risk. However, insurance firms have not been subjected to such engagements leaving a gap in their preparedness in addressing ICT/cyber risks. The proposed guideline is intended to address both banks as well as insurance firms.

10. **Discussion with select banks helped in understanding their preparedness and perception about the extant guidelines.** As part of the mission, to appreciate the banks' view, a meeting was arranged with two major banks—one locally owned and the other owned by a foreign parent. The discussions revealed that banks are considering ICT/cyber risks carefully and have taken various steps to mitigate those risks. It is also seen that one of the banks headquartered at Trinidad and Tobago has several subsidiaries in multiple countries, even beyond Caribbean countries, having to face additional burden of managing the IT services for subsidiaries as well. A foreign bank subsidiary operating locally indicated that most of their IT services are outsourced to their parent located in another country, leaving limited capacity to address such issues locally. Both banks could not recollect the range of regulatory guidelines already applicable to them as these were fragmented. There was willingness to report cyber incidents to the CBTT, but there was reservation in sharing information among peers. This is an area where CBTT can build awareness further.

11. **Discussions with the working group provided key inputs in the preparation of a draft guideline.** As part of the mission discussions were held with the working group to understand the approach being adopted in developing the guideline. In addition to the seminar on

regulation as referred above, guidance also was provided during the meeting on areas like scope and applicability of the guideline, proportionality issue, need to elaborate the instructions where needed based on the local needs, developing technology neutral guideline, and making the guideline outcome focused. It is observed that the burden of developing the guideline is primarily on CBTT team, considering the expertise available with other financial regulators.

12. **Resource constraint is acute in ICT/cyber risk supervision with only one junior examiner earmarked partially for banks and none for insurance and pension firms**. The organizational structure of the FISD indicates responsibilities for supervising banks and nonbanks was entrusted to one division and insurance and pension firms to another. Within banks & nonbanks division, supervised entities are allocated among three teams which are collectively responsible. The practice of assigning a dedicated supervisor even in the case of top five banks is not in vogue. Similar arrangements were there for insurance and pension firms. As per the organizational chart shared with the mission, the number of supervisory staff allocated to the supervision of banks / nonbanks at 16 (includes the manager and administrative assistant) is less than the number of staff available for insurance and pension firm supervision. Among the bank / nonbank supervisors only one Junior Examiner is an IT qualified resource partially marked for such work. Among insurance supervisors, no such resource is available. To provide a perspective, discussions reveal that banks/insurance / pension firms have a share in total assets of 60/20/20 percent respectively.

13. **Leveraging the capacity available at 'Risk Management' and 'Audit' functions of the CBTT for supervisory purposes is useful in the short term.** The current practice of involving ICT/cyber expertise available in staff attached to risk management and audit function is very useful, given the acute shortage of resources within supervision. Such arrangements tend to bring forth several coordination issues and may potentially lead to lack of ownership and control.

14. **Supervisory practices in assessing cyber risk are yet to evolve fully. Currently thematic reviews and surveys play an important role, though such exercises are infrequent.** In respect of banks, FISD has engaged with the banks as part of the regular supervision efforts in assessing IT risks leveraging both external and internal audit work. There are no prescribed testing requirements. RBS manual is dated and requires an update urgently to focus on the ICT/cyber risks, which will be given priority upon completion of the cybersecurity guideline. Periodical surveys (four conducted in the past eight years) provide some input but are not sufficient to appreciate the risk profile of the banking institutions. Onsite supervision focusing specially on ICT/cyber risk and offsite capabilities are very limited.

B. Recommendations

15. **Augment the resources in ICT/cyber risk supervision.** Digitalization of financial services has progressed rapidly, and financial institutions are adopting newer technologies more frequently. Consumer demand for digital services is increasing, propelling financial institutions

to expand their digital landscape. It is therefore necessary to have adequate supervisory resources to focus on this area. Drafting a guideline, consulting with the industry, finalizing the guideline and issuing it will take serious effort. Subsequently, assessing the compliance with the guideline will increase the supervisory burden. The current complement of only one Junior Examiner earmarked for this purpose in respect of banks/nonbanks and no staff for insurance/pension firms suggests that there is an urgent need to augment supervisory resources in ICT/cyber risk supervision.

16. **Draft the guideline on ICT/cyber risk covering banks, insurance companies and pension firms on the basis of various inputs provided in the Seminar on Regulations.** Though banks, insurers, and pension firms are at different stages of maturity when it comes to managing ICT/cyber risks, it would be ideal to include all of them under the scope of the new guideline. If needed, more flexibility could be provided in terms of implementation in respect of insurance and pension firms.

17. **Include a provision in the guideline to conduct an independent periodic assessment of cyber preparedness of banks, insurance companies and pension firms by qualified external professionals.** Given the acute shortage of supervisory resources, in the initial days it will be beneficial to leverage the work of external audit firms. Many jurisdictions require financial institutions to periodically assess their ICT/cyber preparedness with the help of external audit firms and to submit such reports for central bank's perusal.

18. **Incorporate in the guideline a requirement for the Board to identify the regulatory gaps, draw an implementation plan with appropriate milestones, and submit to the CBTT.** The guideline, when issued, will mandate certain new requirements on the part of financial institutions and may need to provide an implementation period given additional investments it may warrant. It is a good practice to require Boards of supervised entities to make an assessment of gaps and draw an implementation plan with milestones to bridge those gaps. CBTT could also consider including requirement for institutions to conduct a gap analysis as a standard requirement for all recently issued guidelines. Such information would be very useful for supervisors in their assessment and when collected on regular intervals will provide an understanding of the progress made by various institutions.

19. **Determine the level of details to be provided in the draft guideline considering the local environment and digital landscape.** Regulatory guideline needs to meet the style and usage expectations of the local environment. While principle-based guideline is welcome, the level of details will depend on the expertise available within the Boards of supervised entities and other local factors. Consider providing sufficient details in the guideline so that the implementation of the provisions of the guideline is facilitated.

20. **Prepare a cyber incident reporting template and require supervised entities to report cyber incidents regularly.** As part of ICT/cyber risk management, it is important to collect information on cyber incidents regularly. Cyber incident reporting offers several benefits

both to the supervisor as well as supervised entities. It is a good practice to integrate such requirements in the guideline.

21. **Sensitize the regulated entities on the need for strengthening cybersecurity through speeches, interviews, etc., and impress upon them the need for cyber incident reporting and information sharing among banks.** The process of drafting the guideline, review, obtaining industry views, finalization, and approval can take up to six months. It is important to prepare the industry for such a guideline as the demands of such regulatory guideline will be substantial on the part of supervised entities. It is often a good practice to sensitize them well in advance by way of top management speeches, interviews to reputed financial dailies, etc.

22. **Plan and conduct ICT/cyber preparedness surveys among insurance companies and pension firms**. The level of preparedness among supervised entities differs. While banks are subjected to thematic reviews, surveys, and virtual assessments on their ICT/cyber preparedness, insurance and pension firms have not been exposed to such supervisory engagements. It is therefore necessary to initiate such exercises for insurance and pension firms. To start with, surveys on ICT/cyber preparedness could be attempted.

23. **Increase the frequency and intensity of ICT/cyber risk assessments, starting with major banks.** Banks are the dominant set of institutions within Trinidad and Tobago in terms of their share of financial system assets and they tend to adopt technology faster. Some of the banks are large entities having many customers and offering various digital services. It is important to increase the frequency and intensity of ICT/cyber risk supervision at least for top banks in the near term.

24. **Plan and augment supervisory resources to ensure a self-sufficient supervision function covering banks, insurance companies, and pension firms.** Considering the varying level of digital maturity of the supervised entities and the number and size of such entities, it is necessary to have sufficient resources within supervision unit to address the emerging ICT/cyber risks. Supervisors also have the responsibility to have a macro perspective, looking at various interdependencies, interconnections, concentration risk, and financial stability implications. The work involved in bringing insurance and pension firms will be daunting as lot of efforts will go in educating and building awareness. Therefore, it is urgent and necessary to augment supervisory resources. This could be seen as an investment rather than expenditure as qualified supervisors would lead to operationally resilient financial institutions in the long run.

25. **Consider setting up an offsite supervision function for ICT/cyber risks.** Basel core principles require supervisors to have a combination of onsite and offsite supervision to effectively supervise banks. ICT/cyber risk supervision also requires offsite supervision capabilities as supervisors need to collect various key performance indicators, cyber incidents—both individual major incidents and summary level information, organizational structure of the supervised entities, digital products, list of third-party arrangements, various test reports and policy documents so that a risk profile or dashboard could be prepared for each of the supervised

entity. Such an arrangement would further facilitate in obtaining a macro picture of the sector. Well-structured offsite capabilities will facilitate more efficient onsite supervision as well.

IV. Cybersecurity Governance

A. Assessment

26. **Cybersecurity governance at CBTT is set up according to generally accepted good practices in the financial sector, with some minor differences.** All three lines of defense—that is, management control, risk management, and internal audit—have cybersecurity capabilities. Resource constraints are apparent in the first line, while those in the second and third lines are less strained.

27. **Unusually, the second line of defense—risk management—has a formal responsibility in driving IT governance.** Most financial institutions have their second line focusing on risk data collection, consolidation, analysis, and reporting, and do not expect it to be operationally involved in IT Governance because IT Governance involves setting up organizational structures and policies and procedures to ensure effective and controlled IT operations. The second line usually does not have this responsibility.

28. **The information security function in the first line is subordinated to the Head of IT.** This arrangement is losing ground in the industry because of the growing importance of cybersecurity and increased risk of conflicts of interest. However, it still has advantages[2] and with appropriate compensating controls, the conflict of interest risk can be mitigated.

29. **Cybersecurity policies and procedures cover the most important topics and have been recently updated.** Missing areas include secure application development standards and security hardening baselines.

30. **Policies governing the cybersecurity of payment systems are uneven in terms of the technical controls required.** The SWIFT cybersecurity control environment is more comprehensive due to the formalized requirements of the CSP.

31. **Regular recovery tests of critical systems are not performed.** Testing to date has been limited to tabletop exercises and has not incorporated tests using services from the disaster recovery site to conduct business operations. In the event the primary site services become inaccessible, the recovery site is presently configured to provide selected services deemed to be critical.

[2] Most notably, closeness to IT operations, which has the largest influence on cybersecurity in an organization.

B. Recommendations

32. **Assess the workload of the IT Security unit and increase resources as needed.** In order to determine the nature and extent of additional resources, an analysis of the unit's current workload should be performed, including operations and project work. CBTT's commitment to improving its cyber resilience will result in additional workload on top of an already stretched agenda, which needs to be estimated and the necessary resource development plans drawn up in advance, as there is a general shortage of available skills. The mission's scope did not include a deeper dive in this area and thus cannot make more specific recommendations. A rule of thumb that might be used to check the reasonableness of resource allocation is that in banking the information security workforce Full Time Equivalent (FTE) is typically in the 10-15 percent range of the IT workforce FTE. Given that the CBTT operates critical infrastructure for the financial sector, the actual ratio may be closer to the upper bound.

33. **Remove IT governance from the responsibilities of the risk function.** The risk function should focus on risk data collection, consolidation, analysis, and reporting and not be involved operationally in governance matters, including IT and cybersecurity.[3] IT and cybersecurity governance is best assigned to the IT department and the IT Security unit respectively, under the direction and oversight of senior management, and subject to review by internal audit. Senior management should require that IT and cybersecurity governance is set according to the broad governance principles adopted by the CBTT and obtain assurance thereof through internal audit.

34. **Establish regular cybersecurity meetings and reporting regime at the Board level with the participation of the Head of IT Security.** This "dotted line" reporting arrangement will act as a compensating control that mitigates the risk from potential conflicts of interest between IT and IT Security management. For example, without such an arrangement IT Security management that is subordinated to IT management might find it difficult to voice opposition to decisions detrimental to cybersecurity. Alternatively, the cybersecurity function could be elevated to the same level in the organization as the IT function.

35. **Develop a secure application development policy and security hardening baselines.** The CBTT does internal (in-house) application development, including security sensitive functionalities. Security vulnerabilities in software often occur because of insufficient focus on secure development practices. A secure application development policy helps reducing the number and severity of such vulnerabilities by mandating, among others, development methods and coding approaches that promote security by design, code reviews, testing for exploitable bugs, and secure configuration of the development toolchain. A related area that needs attention is the strict separation of the development, test and production environments and restricting

[3] The risk function has not been actively pursuing operational involvement in IT or cybersecurity governance in recent times, so the recommendation will not result in any disruption; it will only align the de jure roles and responsibilities with the de facto situation (and good practice).

access of developers to production systems. Finally, security hardening baselines help improving security by mandating configuration settings on servers, workstations, networking devices, etc., that decrease the attack surface.

36. **Develop a policy to bring the cybersecurity controls of the ACH and RTGS systems more in line with the SWIF CSP.** The SWIFT CSP encapsulates the best practice in payment system related cybersecurity control and thus can form a strong basis for improving the cybersecurity of other payment systems as well.

37. **Regularly commission security reviews and tests of the payment systems.** CBTT uses a scanning tool to mitigate the risk posed by unpatched vulnerabilities in its IT environment. Indeed, frequent vulnerability scans and timely patching of the vulnerabilities found are the foundations of effective defense against malicious attacks. For high-risk systems, such as payment systems, this should be augmented with security configuration reviews, including access rights reviews and network security reviews because vulnerabilities may exist that cannot be detected by remote scans. Furthermore, security testing, such as penetration tests, convey additional needed assurance over the effectiveness of cyber defense. The frequency of the reviews and tests should be determined based on the risk tolerance and budgets available. Typically, penetration tests and security reviews of payment systems are done annually, with more frequent (e.g., weekly, monthly, or quarterly) vulnerability scans in between. The minimum requirement for scanning frequency should be quarterly and after any significant changes.

38. **Disaster recovery tests should progress beyond tabletop exercises and include simulating a complete failure in the primary data center**. This would necessitate performing a full recovery using the offsite resources as far as possible. More disruptive tests could be considered after gaining experience, whereby the data center is shut down. Such tests will require extensive preparation and planning and will typically be performed less frequently.

V. Identity and Access Management Project

A. Assessment

39. **The IAM project is set up according to good project management practices.** There is a project charter in place, which documents the goals, stakeholders, sponsors, outline, and deliverables for Phase 1. A project plan is available as well.

40. **The project is in a very early stage; thus, the mission could not meaningfully assess performance and delivery against plans.** A follow-up mission in the first quarter of 2023 would be in a better position to carry out such an assessment. Therefore, the mission focused on sharing experience and good practices and answering specific questions raised during discussions.

41. **The core project team consists of staff from the IT and IT security departments.** The project charter does not specify the time commitments needed form staff, for example in FTEs. The mission cautioned that the workload can be high, and involvement of the business functions is required, especially in the initial stages of the project.

42. **The deliverables for Phase 1 are clearly identified and creating them within the deadline seems feasible.** Phase 1 ends on January 31, 2022. As a key activity in Phase 1 some of the potential vendors have been contacted for general information. A review of the IAM policy is scheduled, as well as work on the authoritative source for identity information.

43. **It is unlikely that the budget of TTD 100,000 (approximately USD 14,700) set aside for IAM advisory services will be sufficient.** External advisors are often brought in to benefit from IAM-specific subject matter knowledge, methodology and tools, assist in requirements definition, role review and reengineering, solution design, vendor selection, and do quality assurance and post-implementation review. Given the size and complexity of the project, and the going rates for relevant services, the budget could be exhausted by just one of these tasks.

B. Recommendations

44. **Plan out Phase 2 of the IAM project and include requirements definition and roles and access rights review and reengineering as key tasks, among others.** The mission supports the phased approach and suggests that the November 2022 timeframe is ideal to start planning for Phase 2 that should commence in February 2023 and ideally finish in a few months' time.[4] The requirements definition should include functional and non-functional requirements as well. Among the functional requirements, special attention should be paid to those addressing workflow and policy management, interfacing and integration, and search and analytics. Key non-functional requirements include those addressing performance, availability, usability, and security. Security requirements should address logical access and data security controls, and logging and monitoring. The roles and access rights review are necessary to identify inconsistent, conflicting, or missing role definitions, cases of access rights non-compliance with policy. The review also serves as an input to role reengineering, which aims to reduce the number of roles and fine-tune the associated access rights so that the principles of least privilege and need-to-know based data access are adhered to. It is important that the business functions are involved in the role review and reengineering work as they are responsible for setting out the rules for system access within their organizational units, in compliance with applicable policies.

45. **Analyze the projected workload and expertise required vs internal resources and skills to determine the type and extent of third-party support that needs to be sourced.** The total effort needed to deliver the project should be estimated in terms of FTEs (or man-days or

[4] Experience shows that project phases of durations from 3 to 6 months are conducive to a successful project, especially if each phase has clearly identifiable benefits, as frequent delivery of results keep the up the momentum and motivation of the project team.

work hours, whichever is deemed more suitable). The expertise required should be identified as well. Comparing these with the project timeline, the internally available skills, and resources will enable CBTT to better estimate the external support needed, and consequently, the expected outlays. Typically, internal skills in short supply in an IAM project include role reengineering, access rights review, interface development, and system integration.

46. **Adopt a phased approach to IAM deployment.** It is advisable to do the deployment of the selected IAM solution over several phases. This reduces the risk of widespread disruption should unexpected errors occur. The first phase of the deployment (which is not the same as the first phase of the IAM project itself) could be considered a pilot and could include Active Directory and one or two internally developed applications. In this way, operational experience could be gained in a live but limited environment.

47. **Adopt good IAM implementation practices listed in this report as deemed necessary.** Given the early stage of the IAM project several options how to structure and run it are still open. The good practices listed in the Appendix can be used as a guide when making decisions on the actual course of action.

ANNEXES

ANNEX I. SELECTED GOOD IAM PROJECT PRACTICES

The following is a non-exhaustive list of good practices that in the experience of the mission team can significantly contribute to the success of an IAM project. CBTT is advised to decide on the adoption, adaptation, or rejection of any of these based on professional judgment, considering the circumstances of the institution in general, and the project in particular.

1. Requirements and vendor selection

a. Both functional and non-functional requirements are developed, involving representatives of key stakeholders, e.g., IT, information security, and business units.

b. Requirements regarding workflow, interfacing, integration (e.g., with the service desk application), batch processing, analytics, search, and security are prioritized. All requirements are assigned a priority level, e.g., must-have, negotiable, and nice-to-have.

c. Requirements for IAM related services, both from vendors and independent advisors are defined and prioritized. Typical services for consideration include role reengineering, quality assurance, security testing, and post-implementation review.

d. An initial market research is done to identify not more than three to four IAM potentially suitable IAM products/vendors (candidates).

e. A more detailed analysis is done to reduce the number of candidates to (typically) three. At this stage the capabilities, references and reputation of vendors is informally checked.

f. A formal Request for Information (RFI) is issued. Candidates are asked to give presentations, provide test or demonstration licenses, and support a “test drive” of the product.

g. The test drive includes, among others, experimenting with the product features that fulfill the prioritized requirements, and the full identity lifecycle.

h. A formal Request for Proposal (RFP) is issued. Candidates are asked to show not just one-off costs but also the total cost of ownership for several years. Costs are required to be shown according to a template to facilitate comparative analysis.

i. Financial and technical information in the proposal is assessed separately according to predefined and weighted criteria.

j. A similar, preferably simplified process for selecting independent advisors is in place. E.g., it is rarely necessary to go for separate RFI and RFP phases.

2. Implementation

a. The IAM project raises awareness among, and getting buy-in from, key stakeholders. The project sponsors lend their support and use their authority to promote this effort.

b. The IAM project is treated equally as a business and IT endeavor. The messaging emphasizes the need for the business units to participate, especially in the planning, role review and reengineering, and testing activities.

c. Types of user identities are identified, e.g., human, non-human (service accounts), employee, contractor, supplier, etc. The initial set is consolidated to the minimum necessary. e.g., are there meaningful differences that require separate treatment of full-time and part-time users? Is there a need to differentiate between various types of external (non-employee) users?

d. All systems that users have access to are identified, irrespective of the initial scope of the IAM implementation.

e. An identity and access review are done, at a minimum for the systems in scope for the pilot and the first phase of deployment, preferably including systems in subsequent deployment phases as well.

f. The authoritative source of identity information is identified early in the planning phase. Interfacing and synchronization possibilities are explored as well.

g. If external advisors are used for quality assurance, then they are involved early in the planning phase.

h. A pilot phase is defined, with a limited scope and time span, but including a “difficult” system (typically, an in-house development that has no standard connector to the IAM).

i. Deployment is done in a phased approach and according to a roll-out plan.

j. A roll-back plan is in place.

k. Roll-out and rollback is tested before live deployment.

l. A segregation of duties matrix is used for the IAM system access rights set-up.

m. The IAM infrastructure is security hardened and tested before deployment.

n. A knowledge base is developed as the project progresses towards deployment. Focus is on solutions to issues in the provisioning and lifecycle management process.

o. A post-implementation review is done after the first or second phase of deployment.

ANNEX II. AGENDA – SEMINAR ON REGULATION

Tuesday, November 1, 2022 – DAY 1 OF TRAINING (*in person*)			
9.00 am – 9.15 am (Local time)	**L-0**	**Welcome and Introduction** *CBTT - Mr. Patrick Solomon, Inspector of Financial Institutions* *IMF Staff (Rangachary Ravikumar, Tamas Gaidosch, Mission Chief)*	
9.15 – 10.30	L-1	Cyber Risk and Financial Sector – An Introduction. Cyber Risk and Financial Stability Growing digitalization and interconnectedness, attacks becoming frequent and sophisticated, renewed focus on operational and cyber resilience. Cyber terms explained. Cyber risk and its impact on financial stability, transmission channels	*Tamas Gaidosch*
10:30 – 10:45		**BREAK**	
10.45 – 11.25	L-2	Cyber Security - Overarching Framework National level policy and institutional arrangements, arrangements within central banks and emerging best practices like DORA, etc.	*Rangachary Ravikumar*
11.25 – 12.00	L-3	Cyber Security and New Technologies; Cloud Regulation Adoption of new technologies growing, posing unique challenges for cyber security. Discuss cyber risk implications of adopting AI/ML, fintech, etc. To discuss the importance of cloud and how to regulate.	*Rangachary Ravikumar*
Wednesday, November 2, 2022 – DAY 2 OF TRAINING (*in person*)			
9.00 – 9.50	L-4	International Guidance on Cyber Risk and Global Regulatory Practices – An overview An overview of work on cyber and related topics by standard setters and major regulators	*Rangachary Ravikumar*
9.50-10.45	L-5	Core components of Cyber Risk Regulation – Governance, Risk Management Components of cyber risk regulation and focused discussion on governance arrangements and risk management practices	*Rangachary Ravikumar*
10.45-11.00		**BREAK**	
11. 005 – 12.00	L-6	Outsourcing / Third Party Risk Management / Vendor Risk Management Outsourcing policies, oversight, and best practices	*Tamas Gaidosch*
Thursday, November 3, 2022 - DAY 3 OF TRAINING (*in person*)			
9.00 – 10.00	L-7	Cyber Incident Reporting Cyber incident reporting best practices, reporting frameworks and need for convergence	*Rangachary Ravikumar*
10.00 – 11.00	L-8	Business Continuity & Response and Recovery – Emerging best practices Business continuity management – issues and challenges. Discuss FSB paper on best practices on cyber incident response and recovery, importance of response and recovery within the financial sector.	*Rangachary Ravikumar*
11.00 – 11.15		**BREAK**	
11.15 – 12.15	L-9	Information sharing / testing frameworks – how are they handled in regulations Benefits of gathering threat intelligence and information sharing, examples of best practices	*Tamas Gaidosch*
Wrap Up/ Closing Remarks 12. 15 – 12.30		IMF CBTT	