I. Introduction

1. The CBSI has a clear obligation to manage its risks. Under the CBSI Act the board is responsible for, *inter alia*, "assessing risk and formulating contingency plans for the ongoing operations and security of the central bank."[1] As part of its strategic plan (2020-2024), the CBSI established a Risk Management and Corporate Communications Department (RMCCD).[2] Within this department a Risk Management Unit (RMU) has been created in 2020, staffed initially with two staff, to coordinate risk management, including responsibility for the middle office function. The RMU reports to the head of RMCCD who reports to the deputy governor.[3]

2. Technical assistance (TA) mission objectives and approach. The objective of the mission was to guide the CBSI on defining and articulating its risk management framework, with emphasis on advancing two specific outcomes. The first of these is to work to establish a strong risk culture where the governor and board subscribe to the need for effective risk management, communicate this to the organization, and are clear on what their respective roles and responsibilities are, including of the Board Audit Committee (BAC). The second is to strengthen risk governance, ensuring a member of each first line department (often referred to as a risk champion) is assigned responsibility for coordinating the risk management process, ensuring it is undertaken in a thorough and timely manner to assist the RMU, and the RMCCDs risk staff are clear on their second line responsibility to design and consistently embed risk management across the CBSI. This includes, additionally, the need to ensure that the RMCCD acts to integrate and ensure consistent reporting on risks to the governor, the BAC, and the board in general. The mission objectives were to: (i) review relevant documentation; (ii) engage in pre-discussion with management, governor and Board; (iii) present on (international and regional) risk management best practices for central banks; (iv) provide practical guidance on how the CBSI should advance maturing its risk management capabilities; and (iv) provide directional guidance, setting reasonable milestones for steps forward. This report builds on presentations to leadership and separately to board representatives, guiding on international best practice in risk management for central banks.

II. Risk Management Diagnostic

3. The CBSI has made several important steps in enhancing its risk management. Over the past few years, and with the assistance of the IMF, and its regional training center, the Pacific Technical Assistance Center (PFTAC), the CBSI has sought to improve its financial risk management, particularly in relation to the management of its foreign exchange reserves. Here the CBSI's Reserve Management Framework has been revised with greater focus on avoiding losses and liquidity relative to the prior focus of generating return. The CBSI is developing its operational risk management capabilities, enhancing local risk management for high priority categories of risk, such as information technology, currency management and procurement. Nonetheless, it is evident to the mission that the CBSI's

[1] As outlined under Section 39 of the CBSI Act.

[2] RMCCD was established in 2019.

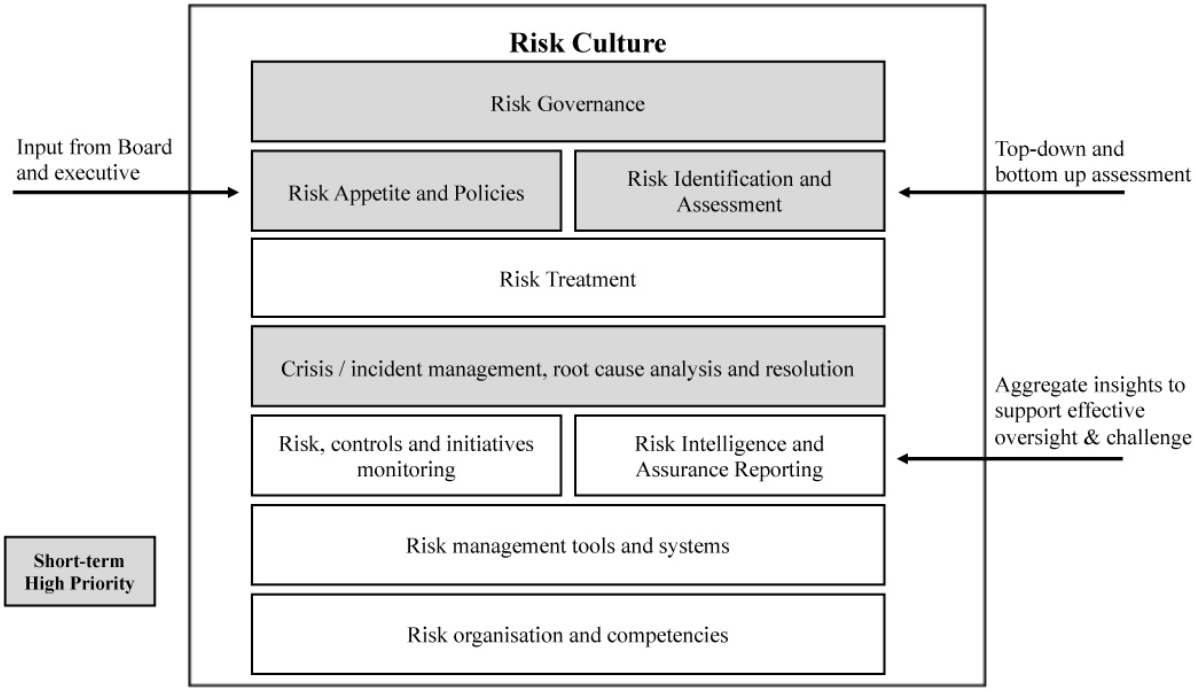
[3] The Deputy Governor is also a member of the CBSI Board. As outlined under Section 39 of the CBSI Act.

approach remains fragmented, resulting in difficulty for either the executive leadership or the board to maintain coherent oversight or assurance that all material risks have been identified and are being managed effectively.

4. The development of an Enterprise Risk Management (ERM) Framework is viewed as a priority by the CBSI. The mission observed strong support across the CBSI for adopting a formal ERM framework. However, to provide a structured and coherent approach to managing risk across CBSI, the ERM Framework will need to be supported by effective risk governance and tone from the top to cultivate a strong risk culture at all levels.

5. ERM is more than a program, a project, a process, or any one unit. It represents the aggregate of the risk governance, risk policies and procedures, integrated risk reporting and risk related skills and competencies. As these are progressively integrated, the approach to risk management becomes self-reinforcing, promoting regular risk dialogue from senior leadership and the board. The ERM Framework can evolve to promote a holistic risk culture, the elimination of risk blindspots and the interlinkage between the strategic plan and risk management can be strengthened. The components of an effective risk framework are illustrated in Figure 1.

Figure 1. Enterprise Risk Framework



Source: Mission

6. The mission recommends a phased implementation of the risk framework, starting with strengthening CBSI risk governance. Given that the CBSI is constrained by limited resourcing of the RMU, it is recommended that the implementation of the framework be phased, with an initial focus on the components shaded in grey in Figure 1 above. It is recommended that the CBSI first strengthen its risk governance, while in parallel refining and enhancing its approach to aggregating risk intelligence from the identification of top-down

strategic and emerging risks and bottom-up operational risks. The strengthening of risk governance will require the RMU to engage with senior leadership and the board to define the risk appetite for the CBSI across material categories of risk. Lastly, it is recommended that the CBSI build on its crisis and incident management capability, by formalizing an Incident Management Team (IMT) capability, building on the approach that the CBSI has developed to govern and manage its response to the pandemic. Overall, this phased approach to implementing the risk management framework will ensure that the CBSI can progress in implementing some of the key foundational blocks of its framework. At the same time, this approach would also acknowledge the scale and CBSI resource constraints, reinforceing the critical importance of risk governance and ensuring a continuous, organization-wide contribution to safeguarding the CBSI and its efforts to meet its legal objectives.

III. Risk Governance

A. Current Situation

7. Effective risk governance must encourage a full understanding, dialogue and constructive challenge on the organizational risks. Risk governance relates to the quality, independence and reliability of the internal processes adopted by the CBSI to manage all of its risks. As such, risk governance encapsulates not only the role, responsibilities and functioning of the board and its executives in relation to risk governance, but also the adequacy of the internal structures, operational controls and procedures to manage risk throughout the organization. Importantly, effective risk governance must support effective decision making, including the allocation of limited CBSI resources.

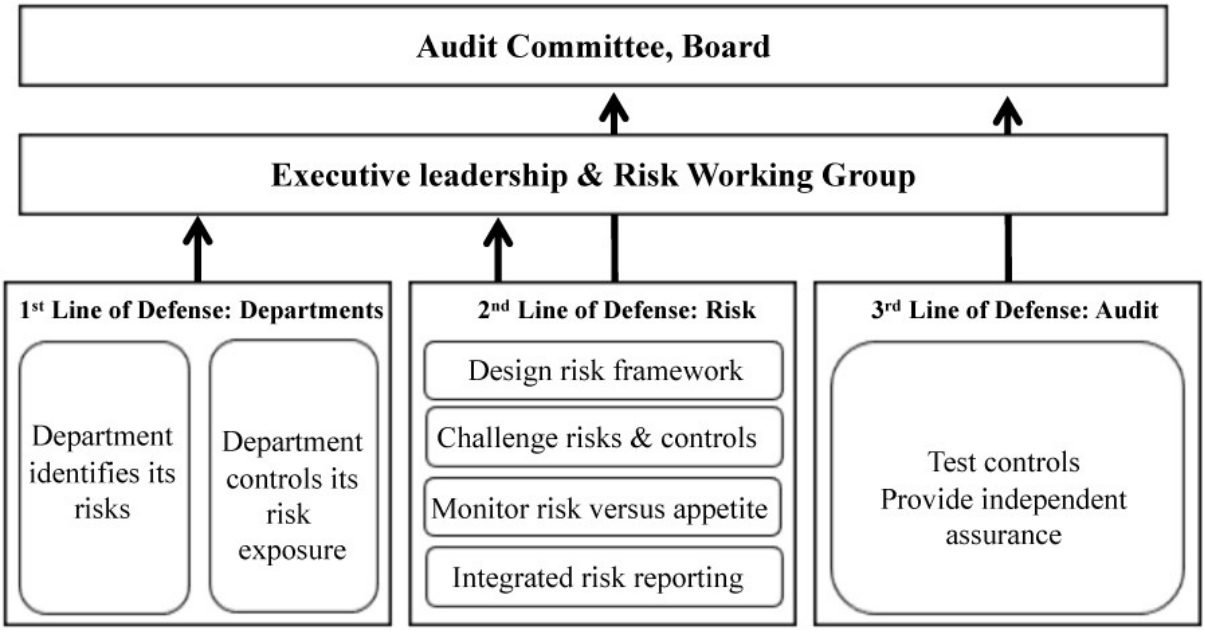
8. The CBSI's risk governance is currently weak. There is no recurring review of the broad spectrum of risks that confronts the CBSI on an ongoing basis. Rather, to date the executive and board have reviewed specific policies on a point or somewhat *ad hoc* basis. The absence of structured risk and incident reports results in infrequent dialogue and an inability for both executive and board to have transparent, tailored oversight to align on the most material risks and to maintain frequent oversight to ensure risks are mitigated on a prioritized basis. It is also evident there is a governance gap between first line departmental management and the board; that is, currently there is no executive oversight working group that fosters dialogue to ensure the management teams across the CBSI are aligned on the most material risks. Additionally, there is opportunity for CBSI to consider how the risk intelligence developed by the RMU can be leveraged by internal audit, to support the third line of defense in its role in providing independent assurance on the effectiveness of the control environment.

B. Recommendations

9. Adopt the Three Lines of Defense model of risk management. With rare exception, central banks across the globe have adopted the so-called Three Lines of Defense model, implementing it to integrate into their respective organizational and governance structures. Under this model each department constitutes part of the first line of defense, with responsibility for identifying and managing risks; that is, the first line of defense own the respective risks under each of the management team's local remit. Those risk management

staff (in the CBSI's case, the RMU) that design and coordinate the implementation of the organization-wide risk management framework represent the second line of defense. The second line is also responsible for aggregating the risk information and ensuring it is presented in a manner that provides coverage of all material risks and facilitates the ease at which senior stakeholders and the board can pinpoint and challenge the most material risk exposures. The third line, represented by internal and external audit test to ensure that controls are operating effectively and provide independent assurance on the efficacy of the control environment. For central banks, policy risks are generally managed outside of the formal three lines of defense model, by ensuring effective governance structures are in place that facilitate open dialogue and debate on policy options.

Figure 2. Three Lines of Defense



Source: Mission

10. Clearly define risk management roles and responsibilities. The Risk Management Framework should be drafted, reviewed, and approved by the board. This can take account of the phased approach to implementation as recommended by the mission team. The risk management roles and responsibilities, aligned with the Three Lines of Defense model should be clearly outlined. This should include ensuring a member of each department (or risk champion) be assigned responsibility for coordinating the risk management process, ensuring it is undertaken in a thorough and timely fashion. This will help ensure that each department is effectively discharging its first line of defense responsibilities and supporting the risk reporting back to the RMU, such that it can aggregate the organization-wide perspective.

11. Ensure adequate resourcing of the second line risk management function. Establishing an effective risk culture, supported by robust risk governance, will require top-down leadership sponsorship of RMU. This includes a need for adequate resourcing and training of the risk management staff to support the implementation of the recommendations as set out in this report, along with ensuring the second line risk management staff have the

capacity to operationalize the risk management analysis and reporting required in order to provide support for leadership to maintain governance oversight of risks on a quarterly basis.

12. Establish a Risk Working Group (RWG). The mission team observed a governance gap in that there is currently no regular executive level governance committee or working group that maintains ongoing oversight of the CBSI's risk profile. It is recommended that a Risk Working Group be established, chaired by the deputy governor. Its main objectives would be to maintain oversight on the accuracy of risks being identified, both top-down and bottom-up, and to align on the aggregate risk profile, supporting the RMU with its role to provide aggregate oversight of material risks to the board. The role of the RWG is to: (i) review the RMU's aggregation of the risk inputs provided by each department; (ii) to provide constructive challenge to ensure clear understanding of each risk; (iii) to support the RMU in defining appropriate risk thresholds to recommend to the board in the CBSI risk appetite; (iv) to ensure management options have been considered for material risks; and (v) to ensure that the chosen risk treatment is effectively resourced to enhance CBSI risk management and control. RMU staff should act as secretariat for the RWG, with management representatives from key first line departments. The output should include agreed minutes and actions that ensure risk treatment can be progressed on a risk prioritized basis and reported to the broader executive and board.

13. Include risk management as a recurring item on the executive and board agendas. There is a requirement for structured and quarterly oversight of risk both by the executive and board. There are two simple drivers for this, firstly risk management is a core enabler to the successful execution of any strategic plan, and secondly risk management considerations form an important input into decisions on CBSI resource allocation. As such, the executive must ensure it understands the risk profile and buy into the proposed risk mitigation priorities, prior to the integrated risk report being presented each quarter to the board. The minutes and action log from the RWG should also be provided to the executive and board for information.

14. Include risk oversight in the terms of reference for the Board Audit Committee (BAC). In the implementation and embedding of the Three Lines of Defense model of risk management, central banks typically separate out second line oversight to a Board Risk Committee separate from the Board Audit Committee. However, due to scale and practicality constraints an initial step for CBSI would be to amend the terms of reference for the BAC to support splitting the meetings into agenda items for both risk and control oversight. It is suggested that an effectiveness review survey of the BAC in its oversight of risk be completed at the end of the first year. Clearly, the RMU and Internal Audit should regularly share risk and control insights, to ensure as integrated and coherent an approach to risk and control management across CBSI as possible.

IV. Risk Appetite and Tolerances

A. Current Situation

15. There is currently no defined, board-approved risk appetite. The absence of a clearly defined and board-approved risk appetite or associated risk thresholds, results in the

management team within each department implicitly setting their own risk appetite, which may or may not be aligned to the preferred risk appetite of the executive and board. This weakens consistent and effective internal risk governance, as no *ex ante* standard has been articulated within which management must manage the overall organization. A formal risk appetite would articulate the tolerance levels that the CBSI is willing to accept in the pursuit of its mandate and associated business objectives. As such, the risk appetite is a statement of intent on how CBSI's mandate will be delivered within clear risk parameters—and should therefore also be discussed in and approved by the board. A Risk Appetite Statement (RAS) defines the approach to managing strategic, financial and operational risks, including the sub categories of each. A risk tolerance is then set for each sub category which represents a series of risk limits, set with the intent that they should not be breached, and to support escalation and enhanced oversight if risk exposures are at the upper limit or are breached for a short period of time.

16. The absence of a risk appetite results in inconsistent approaches to specific categories of risk. The current approach to risk management results in inconsistent management of specific categories of risk. For financial risks, for example, and in particular those associated with the investment of foreign exchange reserves, there is a stronger implicit understanding of the risk appetite, and further work has been progressed in articulating the associated policies and approach to oversight. In addition, there has been progress in the structured approach to the management of IT security over the past year or so, including the appointment of a Chief Information Security Manager. However, without formally articulating the broader risk appetite, the CBSI has not considered its approach to proportionately setting thresholds for specific categories of risk. A formal, board-approved risk appetite is all the more important in the context of constrained resources, as it facilitates greater ease of maintaining clear line of sight over those categories of risk that should be tightly controlled versus those where the appetite can be set to be less conservative.

B. Recommendations

17. Formally articulate the Risk Appetite Statement. The RAS should clearly separate out each major risk category and define the risk appetite for each, which should include specific risk tolerances for significant sub categories of risk. The RAS can consider the risk appetite over different time periods, such as short term (up to one year) and longer term, such as within the timeline of the strategic plan. Within the RAS, the CBSI can clarify 'state dependent' constraints, such as how its responsibility as lender of last resort could impact overall balance sheet risk. The RMU should coordinate the drafting of the first version of the RAS, but with input from the RWG, governor and the board. The RAS should have an annual governance review.

18. Gradually calibrate the integrated risk reporting to mirror the structure of the RAS. As the RMU matures the organization's risk reporting, it should be structured to mirror the categories of risk and provide status updates relative to the thresholds as outlined within the RAS. In this manner, it should be possible for board members to quickly determine whether the CBSI is adhering to risk appetite, those risk categories where risk exposures are close to its appetite, and any where the CBSI is in breach. This recommended approach also

enables the executive and board to take a higher level perspective, rather than necessarily having to understand the detail of every risk. As an example, it should be possible to define the threshold or standard to which the CBSI will adhere to for managing fraud related risk, and to provide a simple status update as to whether that standard is being achieved or not. In addition, the approach to risk appetite can allow for the setting of a backstop on the overall distribution of risks, such as setting a limit for the proportion of operational risks that can be categorized as "red," having high impact and high likelihood.[4] In doing so, the CBSI can seek to ensure it is not running too many material risks in parallel.

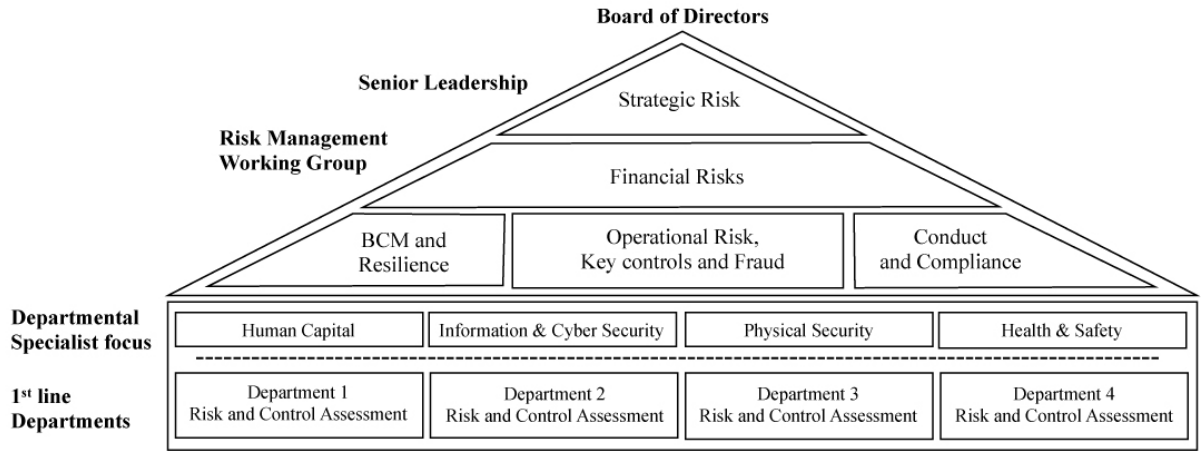
V. Risk Identification and Assessment

A. Current Situation

19. The approach to risk management leverages bottom-up analysis. A traditional approach to risk management focuses on the bottom-up assessment of risks within each risk department, with the risks, existing controls and proposed action plans recorded in each individual departmental risk register. Within the CBSI, the approach to this bottom up analysis is not yet consistent, with risks being articulated differently, which can make it difficult to clearly delineate between risk types and controls and the materiality of each.

20. A bottom-up approach alone results in risk blindside. Under this approach there can also be insufficient consideration of the inter-relationship between risks and incidents. As such the review of a single operational risk may not be the "call to action" that may be warranted if a broader thematic analysis of how equivalent risks manifest across the organization is considered. This is particularly evident for those risks that traverse multiple departments or the entire organization, such as those related to conduct, business continuity, or which have a more strategic dimension. The bottom-up approach is also weak for identifying forward-looking or emerging risks which may not naturally map to a specific department. A risk ownership blindside can therefore emerge.

Figure 3. A Multi-layered View of Risk

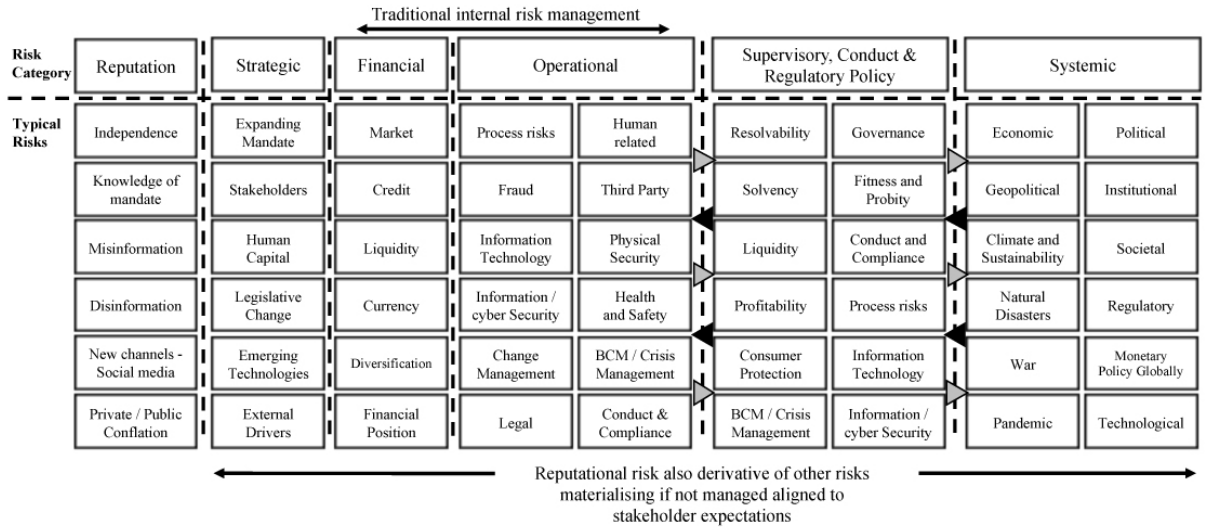


Source: Mission

[4] During the mission's engagements, an example was provided of setting the backstop threshold for operational risks graded as "red" to 5 percent or less.

21. Reinforce the bottom-up approach with a top-down strategic risk assessment (SRA). A top-down approach seeks to ascertain from senior and executive management and the Board their views on the top strategic risks that could impact the organization achieving the delivery of its mandate and strategic plan. As such this top-down perspective can help to integrate risk management with strategic planning, supporting better decision making regarding risk prioritization. This more strategic focus also facilitates the potential exploitation of internal hedges, such as increasing "fail forward resilience" and organizational agility. A clearer end to end perspective on the risk profile can be achieved through combining this top-down risk identification assessment with the risk insights aggregated from the bottom-up operational risk assessments, as illustrated in Figure 3. This approach will better guide the organization on taking prioritized action in managing risk across its risk universe, which is particularly important given the breadth of risk exposures confronted by a central bank, as highlighted in Figure 4 below.

Figure 4. Risk Universe



Source: Mission

B. Recommendations

22. Formalise the approach to risk identification and assessment. The risk identification and assessment component represents an important component of the overarching risk framework that the CBSI should seek to refine and stabilize early in its journey to coherent ERM. Developing and communicating a standard approach that clearly delineates between the assessment of risk with a bottom-up operational focus with departmental management, and a top-down strategic assessment with senior leadership and board is a fundamental enabler for effective risk management. The articulation of this component will outline the methodology for integrating both perspectives, the governance and alignment on priority risks, and define a common language for grading risks based on impact and likelihood.[5] The approach can also define a common template for risk and

[5] See guidance template in Appendix V.

incident reporting by departments to the RMU, facilitating ease of aggregating into a higher level perspective and a standard approach and guidance for root cause analysis for incidents.

23. Align leadership and the board on the frequency of the Strategic Risk Assessment. A common methodology used for an SRA is to use a Delphi-style interview methodology, which can include open-ended surveying of senior leadership and board representatives to ascertain their views on the most strategic and emerging risks confronting the organization. These views can then be probed through a second round of questioning. In addition, it is worthwhile filtering the views by the RMU considering the inputs alongside other external risk intelligence, including broader industry trends.

VI. Other Recommendations

A. Risk Culture

24. Cultivate risk culture at all levels. As noted in Figure 1, risk culture is itself a core component of effective risk management. An organization can develop its risk management framework and policies, but these must be embedded by all staff and consistently reinforced through effective governance and tone from leadership. Therefore, ongoing communication of the development of the risk framework is required, in order to align management and staff to coherently support the risk management journey. The risk culture must foster an environment where management and staff feel safe to identify risks and to report incidents. In fostering the risk culture, the focus should be to cultivate a sense of openness with regard to risk dialogue, where the objective is to iteratively strengthen the approach to managing the risk profile to safeguard the organization. Staff should both understand their departmental risk registers and be incentivized to contribute to refining the articulation of any risks, to register new risks, and to suggest improvements to the control environment.

25. Guide board, leadership and staff through ongoing risk seminars and training. As the risk management framework is developed and implemented on a phased basis, it is critical that the organization is trained to leverage it. At the staff level, a key to success will be the consistency to which the framework components are implemented at departmental level. For risk identification, assessment, and incident reporting, this requires an ongoing cycle of training to departments. Here, there is also merit in RMU advising departments and staff how risk intelligence is being used by senior leadership and the board, given a resource constrained RMU will be heavily dependent on departments submitting quality risk updates for the integrated risk reporting. The risk culture will be significantly influenced by the decisions of senior leaders and their actions which signal the organizational expectations with regard to risk management. If the appropriate tone from the top on risk management is set by the board and senior leadership, it will ultimately cascade down and be sustained by employee behaviours. RMU can also reinforce coherence through the processes it uses in collating risk data and through the timeliness and usefulness of the risk processes, templates for departments to complete and the risk reports provided to the RWG and to executive leadership and the board.

26. Engage with external peers. There is an opportunity for the CBSI to share information on its progress and experiences on risk management with other central banks on

a bilateral basis. In this manner CBSI can gain valuable insight into the risk management framework of peers, building on its earlier regional interactions with the Reserve Bank of Fiji, but also engaging with central banks in other regions, the International Operational Risk Working Group (IORWG),[6] and the possibility of the IMF's PFTAC facilitating further regional information-sharing on central bank risk management. Such engagement will support CBSI in monitoring the maturity of its risk management framework relative to other central banks and monetary and supervisory authorities internationally.

Figure 5. Risk Culture

Source: Mission

B. Crisis, Continuity, and Incident Management

27. Formalize the governance and procedures for crisis, continuity and incident management. The mission observed an opportunity to mature the CBSI approach to the governance of crisis, continuity and incident management. As noted earlier, crisis and continuity management is a risk management discipline that should traverse the organization and which the CBSI has recently developed some competence, given its response to the pandemic. The mission recommends that a core Incident Management Team (IMT) be established, which meets once per quarter to exercise to maintain readiness to respond to any critical incidents. These response procedures would benefit from taking an organizational perspective for such critical incidents, to supplement a standardized RMU defined reporting process to log and act on the learnings from lower level incidents related to specific processes at a departmental level. In doing so, the CBSI would benefit from more tightly coupling its response capability, including the potential to strengthen its management of communications with internal and external stakeholders during a crisis or critical incident. The CBSI representatives provided positive feedback on the role that the Pandemic Task Force had played over the past eighteen months. There is opportunity to build on the lessons learnt and to formalize the governance of crisis and incident management for the longer term.

[6] The IORWG has been established for 16 years and is a center of competence for operational risk management for central banks, and monetary and supervisory authorities.

VII. Concluding Remarks

28. A phased strengthening of risk governance, supported by implementing some core foundational risk management framework components. The recommendations, including strengthened oversight, ensuring risk is a recurring agenda item for the Board (including its BAC) and executive, supported by the establishment of the RWG, and the phased implementation of the combined risk identification methodology (bringing bottom-up and top-down risk perspectives together), with a defined Risk Appetite Statement, with status updates provided in the RMU's regular risk reporting, will significantly advance the CBSI's ERM journey. There is an obligation on CBSI leadership to ensure that RMU is appropriately resourced to progress with the implementation of the recommendations within the timeframes outlined. It will also be important to ensure senior leadership representation on the RWG, combined with strengthening the tone from the top and risk oversight from the board.

29. Follow-up TA. A follow-up technical assistance mission is tentatively foreseen for six to nine months from the start of this mission, with a focus on examining to what extent the CBSI have been able to implement the mission's recommendations and to provide follow-up guidance and support as appropriate. An interim check-in should be completed within three months of the mission concluding, to provide timely feedback to CBSI on any follow-up queries arising as the recommendations are being implemented.

APPENDIX I. DOCUMENTS REVIEWED OR CONSULTED BY THE MISSION

#	Document Title	Date of Issue	Description
1	Central Bank of Solomon Islands Act	2012	The enabling legislation for the Central Bank of Solomon Islands.
2	Public Finance and Audit Act	1996	The act provides for the control and management of public finances in the Solomon Islands. It covers the collection and payment of public monies, the regulation of public debt and the powers of the auditor general.
3	Financial Institutions Act	1998	The act covers the licensing and supervision of financial institutions in the Solomon Islands.
4	Credit Union Act	1986	The act regulates the operations of credit unions in the Solomon Islands.
5	Insurance Act	1986	The act regulates the operations of insurance businesses in the Solomon Islands.
6	Exchange Control Act	1977	The act confers on the central bank the powers of making regulations and imposing duties and restrictions on foreign exchange.
7	Board Audit Committee Terms of Reference	July 2012	The terms of reference of the CBSI Board Audit Committee.
8	Internal Audit Charter	July 2012	The charter describes how the CBSI's internal audit function will undertake its assurance and consulting activities.
9	CBSI Strategic Plan 2020-2023	October 2019	The four-year strategic plan provides an operational roadmap for the bank to meet its mandate over the next four years.
10	Foreign Exchange Department Policy and Operation Manual	June 2000	The document relates to the administration of the Exchange Control Act, the investment of the bank's external reserves and the settlement of the CBSI's international payments by the Foreign Exchange Department.
11	Solomon Islands Information Sharing Mechanism	-	The document sets out the information sharing responsibilities of participants covered by the Solomon Island's exchange control requirements.
12	Exchange Control Manual	-	Covers administration of the Exchange Control Act and associated regulations.
13	CBSI Legal Compliance Policy	-	The policy seeks to ensure that the central bank's operations are conducted in accordance with relevant legal obligations, and to encourage proactive and accountable management.
14	CBSI Procurement Policy	Oct 2020	The policy outlines the procurement standards and procedures that need to be adhered to by staff engaged in procurement to ensure that the bank

#	Document Title	Date of Issue	Description
			gets the value for money in the procuring of all works, supplies and services.
15	CBSI Cybersecurity Policy	Oct 2020	The policy provides a set of rules and guidance to protect the bank ICT network infrastructure and information assets from adverse cyber threats and minimize the cyber risks the bank is exposed to.
16	CBSI Reserve Management Policy and Investment Guidelines	Sep 2017	The document details the policy relating to reserve management, including its governance, the principles for managing reserves, risk management and internal organization.
17	CBSI AML/CFT Policy	Sep 2020	The policy sets minimum requirements and measures for the CBSI and its employees to comply with AML and CFT legislation and the global standards on AML and CTF and proliferation financing activities (CPF).
18	CBSI Business Continuity Plan (draft)	-	The draft plan outlines how the CBSI will respond to, and recover from, business disruptions.
19	CBSI IT Disaster Recovery Plan (Version 2.0)	-	The plan sets out how the CBSI will respond to a situation whereby the normal operation of its computer network system is compromised.
20	CBSI Board Minute No. 8-20	Sep 2020	Extract of board minutes relating to policies on cybersecurity and training and development.
21	CBSI Board Minute No. 9-20	Oct 2020	Extract of board minutes relating to review of risk management-related policies.
22	CBSI Board Audit Committee Minutes – Meeting No. 1	Mar 2020	The minutes of the CBSI Board Audit Committee, including a discussion of the matters arising register.
23	CBSI Board Audit Committee Minutes – Meeting No. 2	Jun 2020	The minutes of the CBSI Board Audit Committee, including a discussion of the matters arising register.
24	CBSI Board Audit Committee Minutes – Meeting No. 2	Oct 2020	The minutes of the CBSI Board Audit Committee, including a discussion of the matters arising register.
25	IMF Technical Assistance Report: Solomon Islands – Foreign Exchange Reserve Management	Apr 2021	A report prepared by IMF technical experts on foreign exchange reserve management at the CBSI.

APPENDIX II. LIST OF PEOPLE MET

The mission met with the following staff and Board members of CBSI:

Governors
Dr. Luke Forau, Governor
Raynold Moveni, Deputy Governor

Board
Christina Lasaqa, Non-executive Director, Member of the Board Audit Committee
David K.C. Quan, Non-executive Director
Bob Pollard, Non-executive Director

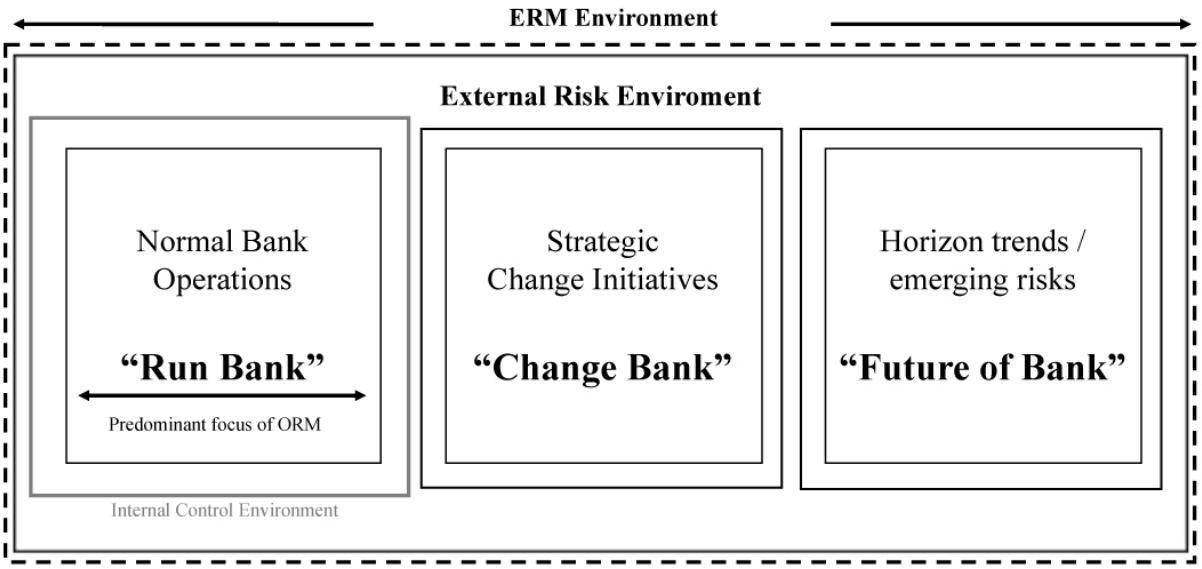
Governor's Office
Marlon Houkarawa, Management Advisor, Operations
Michael Kikiolo, Management Advisor, Policy

Management
Edward Manedika, Chief Manager, Information and Communication Technology Department (ICTD)
Joe Vasuni, Chief Manager, Currency, Banking and Payments Department (CBPD)
Daniel Haridi, Chief Manager, Financial Supervision and Regulations Department (FSRD)
Ali Homelo, Chief Manager, Financial Markets and Exchange Control Department (FMECD)
Emmanuel Gela, Chief Manager, Finance and Accounts Department (FAD)
John Bosco, Chief Manager, Human Resources and Corporate Services Department (HRCSD)
Jimmy Sendersley, Director, Solomon Islands Financial Intelligence Unit (SIFIU)
Louisa Baragamu, Chief Manager, Economics Research and Statistics Department (ERSD)
Linda Folia, Manager, National Financial Inclusion Unit (NFIU)
Oliver Karoa, Manager, Internal Audit Unit (IAU)
Sonia Marahare, Chief Manager,Risk Management and Corporate Communications Department (RMCCD)
Charles Kuper, Manager (Acting), Risk Management Unit (RMU)
Lynne Suti, Analyst, RMU
Uriel Matanani, Manager, Corporate Communications Unit (CCU)

APPENDIX III. SCHEDULE OF VIRTUAL MEETINGS

#	Session	Date	Duration (hours)
1	Meeting with the internal audit and risk management areas	17 Aug 2021	1
2	Meeting with the business units	25 Aug 2021	1
3	Meeting with a member of the Board Audit Committee	26 Aug 2021	1
4	Meeting with the Governor and Deputy Governor	31 Aug 2021	1.5
5	Meeting with the CBSI Board of Directors	7 Sep 2021	1
6	Concluding Session with the Management Committee Members	17 Sep 2021	1.5

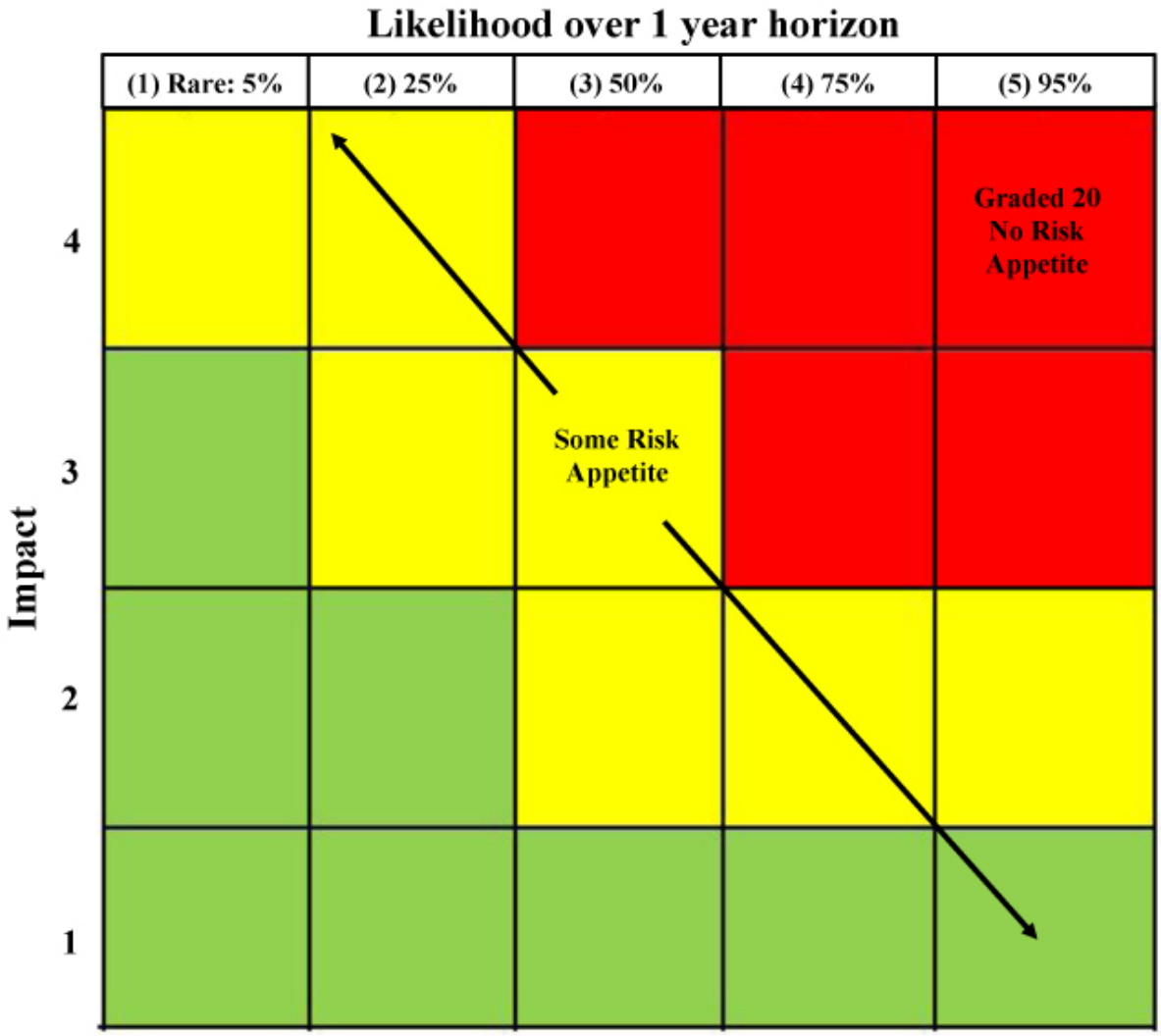
APPENDIX IV. A SIMPLIFIED RISK LANDSCAPE



Experience completing top down risk assessment highlights significant risk 'blindside' in utilising a bottom-up approach such as ORM, BCM and resilience tools alone.

Source: Central Bank of Ireland

APPENDIX V. RISK MEASUREMENT—ORM



Source: Central Bank of Ireland

APPENDIX VI. ERM PRINCIPLES (COSO)

Governance and Culture	Strategy & Objective Setting	Performance	Review and Revision	Information, Communication and Reporting
1. Exercises Board Risk Oversight 2. Established Operating Structures 3. Defines Desired Culture 4. Demonstrates Commitment to Core Values 5. Attracts, Develops and Retains Capable Individuals	6. Analyses Business Context 7. Defines Risk Appetite 8. Evaluates Alternative Strategies 9. Formulates Business Objectives	10. Identifies Risk 11. Assesses Severity of Risk 12. Prioritises Risks 13. Implements Risk Responses 14. Develops Portfolio View	15. Assesses Substantial Change 16. Reviews Risk and Performance 17. Pursues Improvement in Enterprise Risk Management	18. Leverages Information and Technology 19. Communicates Risk Information 20. Reports on Risk, Culture, and Performance
Risk management is a core responsibility of the Board, leadership, management and all staff				

Source: Central Bank of Ireland

APPENDIX VII. TOP-DOWN RISK TEMPLATE

Strategic risk	High level description of risk
Risk and impact description	More detailed articulation of the risk and how it would impact the Bank in the event it materialises
Map to strategic plan	Outline how the strategic risk maps back to the current strategy
Map to objective	How could the risk impact the achievement of mandate or delivery of a core objective?
Impact rating	Rate the strategic risk from low to very severe (if it is really strategic in nature, it will be unlikely to be graded as low)
Impact probability	Assign a probability of the risk materialising
Velocity	How quickly could the risk adversely impact the Bank? Example - cyber security risk = high (immediate), policy risk = medium velocity
Risk type	Endogenous or exogenous? Is it driven by external environment? Controllable?
Maturity of remediation	If the risk is already known or materialising, how does the Bank perceive the effectiveness of the current approach to remediation?
Stakeholder observations	Provide anonymised examples of what stakeholders interviewed have raised in relation to the risk

Source: Central Bank of Ireland