



TECHNICAL ASSISTANCE REPORT

SOLOMON ISLANDS

Central Bank Risk Management

February 2026

Prepared By

Paul Woods (Short-term expert) and Chris Aylmer (Short-term expert)

Authoring Departments/Institutions

**Monetary and Capital Markets
Department**

The contents of this document constitute technical advice provided by the staff of the International Monetary Fund to the authorities of the Solomon Islands (the "CD recipient") in response to their request for technical assistance. Unless the CD recipient specifically objects to such disclosure, this document (in whole or in part) or summaries thereof may be disclosed by the IMF to the IMF Executive Director for Solomon Islands to other IMF Executive Directors and members of their staff, as well as to other agencies or instrumentalities of the CD recipient, and upon their request, to World Bank staff, and other technical assistance providers and donors with legitimate (see [Staff Operational Guidance on the Dissemination of Capacity Development Information](#)). Publication or Disclosure of this report (in whole or in part) to parties outside the IMF other than agencies or instrumentalities of the CD recipient, World Bank staff, other technical assistance providers and donors with legitimate interest shall require the explicit consent of the CD recipient and the IMF's Monetary and Capital Markets department.

The analysis and policy considerations expressed in this publication are those of the IMF's Monetary and Capital Markets Department.

International Monetary Fund, IMF Publications
P.O. Box 92780, Washington, DC 20090, U.S.A.
T. +(1) 202.623.7430 • F. +(1) 202.623.7201
publications@IMF.org
IMF.org/pubs

Acknowledgments

The mission team wishes to express its appreciation to the leadership, management, and staff of the Central Bank of Solomon Islands (CBSI) for their cooperation, constructive engagement, and the time devoted to the mission. In particular, appreciation is extended to Charley Kuper, Manager of Risk, for coordinating the mission's meetings and for providing the team with relevant documentation and background information on the CBSI.

Contents

Acknowledgments	3
Glossary	5
Preface	6
Executive Summary	7
I. Introduction	9
II. Progress Evaluation	9
III. Assessment of Previous Recommendations	13
IV. Other Observations	20
A. Implementation of the Three Lines Model of Risk Management	20
B. Risk Appetite	21
C. Risk Identification	22
D. Incident Reporting	23
E. Business Continuity	24
V. Next Steps	25
VI. Concluding Remarks	26
Figures	
1. Risk Management Framework: Observations	11
2. The Three Lines Model of Risk Management	20
3. Business Continuity Management	24
4. Actions	25
Tables	
1. Recommendations from the October 2022 Report	13
2. Recommendations from the August 2024 Report	18
Annexes	
I. List Of People Met	28
II. Schedule of Meetings	30
III. Documents Reviewed or Consulted by the Mission	31
IV. Virtual Follow-ups	32

Glossary

AML/CFT	Anti-Money Laundering/Countering the Financing of Terrorism
BARC	Board Audit and Risk Committee
BCM	Business Continuity Management
BCMP	Business Continuity Management Policy
BIA	Business Impact Analysis
CBDC	Central Bank Digital Currency
CBSD	Currency and Banking Services Department
CBSI	Central Bank of Solomon Islands
CRO	Chief Risk Officer
ERM	Enterprise Risk Management
ERMP	Enterprise Risk Management Policy
ERSD	Economics, Research & Statistics Department
FAD	Financial & Accounts Department
FIU	Financial Intelligence Unit
FMECD	Financial Markets & Exchange Control Department
FSDPD	Financial Systems Development & Payments Department
GO	Governor's Office
HRCSD	Human Resources & Corporate Services Department
IAU	Internal Audit Unit
ICTD	Information and Communication Technology Department
IMT	Incident Management Team
IRR	Integrated Risk Report
MCM	Monetary and Capital Markets Department
NIST	National Institute of Standards and Technology
ORM	Operational Risk Management
RAS	Risk Appetite Statement
RMC	Risk Management Committee
RMCCD	Risk Management & Corporate Communications Department
RMU	Risk Management Unit
SIFIU	Solomon Islands Financial Intelligence Unit
SINPF	Solomon Islands National Provident Fund
SOLATS	Solomon Islands Automated Transfer System
SRA	Strategic Risk Assessment
TA	Technical Assistance
TLM	Three Lines Model

Preface

At the request of the Central Bank of Solomon Islands (CBSI), the Monetary and Capital Markets Department (MCM) conducted a technical assistance (TA) mission on central bank risk management from July 21–25, 2025. The mission was led by Paul Woods (MCM Short-Term Expert, Central Bank of Ireland) and Chris Aylmer (MCM Short-Term Expert, formerly with the Reserve Bank of Australia), and backstopped from headquarters by Ashraf Khan (MCM, Central Bank Operations Division).

The mission's purpose was to provide technical support and guidance to CBSI in further strengthening its risk management through the development of an Enterprise Risk Management (ERM) Framework. This work builds on the findings of the 2020 IMF Safeguards Assessment of CBSI, which identified the need to enhance risk management practices. It also followed subsequent MCM engagements, including a virtual mission finalised in October 2021, an onsite mission in August 2023, and quarterly technical follow-ups conducted by one of the short-term experts.

The objective of the July 2025 onsite mission was to conduct an independent assessment of CBSI's progress in implementing recommendations from the previous reports. In addition, the mission team provided technical guidance on selected areas, including implementation of the Three Lines Model, business continuity management, and good practices for interaction with internal audit. These activities were intended to support CBSI maturing its enterprise risk management to better safeguard the organization and to contribute to strategic decision-making.

As part of its work, the mission team engaged extensively with senior CBSI stakeholders. Meetings were held with Dr. Luke Forau (Governor), Mr. Raynold Moveni (Deputy Governor), and Mr. Joshua Tuasulia (Independent Member of the Board Audit and Risk Committee). A complete list of CBSI officers who participated in the meetings is provided in Appendix I, and a detailed record of the meetings is included in Appendix II. In addition, the mission team undertook a desktop review of relevant documentation, with a list of the reviewed materials provided in Attachment III. A summary of the quarterly technical follow-up calls is presented in Attachment IV.

Executive Summary

Background and previous assistance. The CBSI requested IMF support for the development of its enterprise-wide risk management framework, building on the findings of the 2020 IMF Safeguards Assessment, which identified the need to strengthen risk management practices. In response, TA was provided through a virtual mission in August to October 2021, followed by an onsite mission in August 2023. Both missions resulted in a series of recommendations to guide the implementation of an ERM framework. In 2024, CBSI requested further assistance, which was subsequently approved later that year.

Objectives of the July 2025 mission. The most recent mission, conducted from July 21–25, 2025, had two main objectives. First, the mission reviewed CBSI's implementation of the recommendations from the two earlier TA reports, identified areas requiring further progress, and provided guidance as needed. Second, it delivered targeted guidance on specific areas of risk management, notably the implementation of the Three Lines Model (TLM) and business continuity management.

Progress since the last mission. Since the previous TA engagement, CBSI has made modest but nonetheless important progress. The Risk Management Committee (RMC) held its inaugural meeting in September 2022, and in December 2023 the Board approved the Enterprise Risk Management Policy (ERMP), which was formally launched by the Governor in March 2024. A revised draft of the ERMP is now under review and includes a strengthened Risk Appetite Statement. In addition, a draft Business Continuity Management Plan has been prepared and reviewed by the RMC. The Board Audit Committee's charter was amended to include risk oversight, and the body was subsequently renamed the Board Audit and Risk Committee (BARC). However, in August 2025 the Board expanded BARC membership to include the Deputy Governor, a step that is not consistent with good governance practice and that risks undermining the essential separation between executive management and Board oversight.

Gaps in the ERM framework. Despite progress, significant gaps remain in CBSI's ERM framework. These include that only basic incident information is provided from departments, the lack of a top-down risk identification process, and an incomplete set of risk tolerances in the draft Risk Appetite Statement (RAS). As a result, senior leadership has not reached alignment on CBSI's overall risk profile and the most material enterprise risks. There is an absence of an integrated risk report to support the effective governance of risk. With insufficient quality risk information, risk oversight has therefore remained limited and incident focused. At present, the BARC relies only on the limited risk information made available to it.

Growing importance of ERM. The need to embed an ERM framework will continue to grow as CBSI faces an increasingly complex operating environment and pursues its digital transformation agenda. A key milestone was the launch of the Solomon Islands Automated Transfer System (SOLATS), the real-time gross settlement system, in April 2024. However, in May 2024, CBSI was subject to a ransomware attack that disrupted internal systems for up to two weeks. A three-year program to address the identified gaps is now underway. This reinforces the need to embed an ERM framework.

Risk culture and oversight Challenges. CBSI's risk culture is showing signs of improvement, but progress remains uneven. The level of challenge from the RMC and the BARC has been limited, incident and risk registers are incomplete, and the approval of new risk-related policies and templates has been slow. Furthermore, some staff remain unclear about their roles and responsibilities under the TLM of risk management. Strengthening the quality of committee discussions and ensuring that risk oversight bodies actively drive risk initiatives will be essential to improving the flow of reliable risk information and insights.

Guidance from the TA mission. During the mission, technical guidance was provided in several key areas: governance and implementation of the TLM, including clarifying expectations for each line of defense and nominating the de facto Chief Risk Officer within CBSI; defining and articulating risk tolerances as part of the RAS; approaches to risk identification; and improvements to the incident reporting regime.

Business continuity planning. Business continuity planning has regained focus at CBSI, underscored by the recent ransomware incident. A draft Business Continuity Management Plan (BCMP) is currently under review. To be effective, the plan should: clearly define governance arrangements and the roles of the RMC, Risk Management Unit (RMU), and responsible departments; outline a structured approach to business continuity; establish a small critical Incident Management Team (IMT); and embed testing and post incident reviews as core elements. The TA mission advised keeping the plan simple, avoiding overcommitment by prioritizing high impact and more probable scenarios in the first instance, and ensuring regular testing.

Commitment and next steps. CBSI has demonstrated a strong commitment to strengthening its risk management practices. It has allocated resources, established an appropriate structure, and resourced its second-line function with a team of three staff. Several initiatives are in progress. However, to embed the framework effectively and generate momentum, these efforts will require strong sponsorship at senior levels, effective risk governance by the RMC and BARC, and should be supported by consistent and frequent communication to management and staff to foster the desired risk culture. Moreover, the Board should reconsider the BARC's composition to maintain a clear and appropriate separation between executive management and Board oversight. A follow-up TA mission is recommended within 18–24 months, incorporating an Executive and Board workshop to assess progress in embedding the ERM framework. This will help sustain momentum, enhance accountability, and reinforce a risk-aware culture across the organization.

I. Introduction

- 1. Background and initial IMF engagement.** The CBSI is seeking to enhance its ERM framework, practices, and processes, while also fostering a stronger risk management culture. Under the CBSI Act, the Board is responsible for “assessing risk and formulating contingency plans for the ongoing operations and security of the central bank.” A 2020 IMF Safeguards Assessment identified the need for CBSI to strengthen its risk management practices. In response, CBSI requested IMF TA, which was provided virtually in August–October 2021, followed by an onsite mission in August 2023.
- 2. Technical assistance reports.** Two TA reports on central bank risk management were produced and published in October 2022 and August 2024. Both reports focused on enhancing CBSI’s risk management approach. The first report set out recommendations to improve risk governance, strengthen specific components of the ERM framework, and support the development of a stronger risk management culture. The second report reviewed CBSI’s progress in implementing those recommendations, provided further advice, and offered more detailed guidance on business continuity management.
- 3. Ongoing engagement and follow-Up.** Following the 2023 TA mission, additional follow-up was arranged through quarterly catch-up calls with IMF short-term experts, who acted as a sounding board for CBSI’s risk management team as it developed key artefacts. These calls took place between April 2024 and May 2025, with summaries reported back to the IMF. Despite this ongoing engagement, progress remained limited, leading CBSI to request further onsite TA.
- 4. Objectives and approach of the July 2025 mission.** The objectives and approach for the most recent TA mission were agreed in advance and had two interrelated goals. The first was to review CBSI’s implementation of recommendations from the two earlier TA reports, identify areas for further progress, and provide supporting guidance as needed. The second was to deliver targeted advice in specific areas, including implementation of the TLM, business continuity management, and effective engagement with internal audit. The agreed approach combined a desktop review of relevant documentation with extensive engagement with CBSI officers, enabling the mission team to assess current practices and progress to date. Building on this assessment, the mission focused on providing practical advice and guidance to support the effective implementation of earlier recommendations.

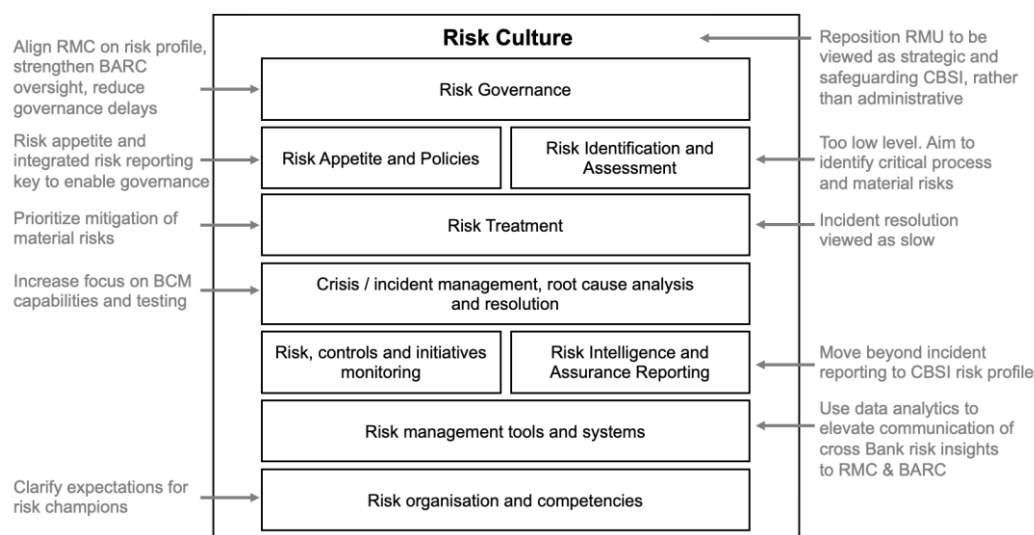
II. Progress Evaluation

- 5. Broad mandate of CBSI.** Like most central banks in the region, CBSI has a broad mandate. Its responsibilities include monetary policy, exchange rate management, the holding and management of foreign exchange reserves, currency issuance, collection and publication of statistics, promoting a safe and efficient payment system, supervising financial institutions, acting as banker, financial adviser, and fiscal agent to the Government, and advancing financial inclusion. The Bank’s mandate is expected to broaden further as the Government reviews legislation on AML/CFT, credit reporting, and financial supervision.
- 6. Transformational change agenda.** CBSI’s vision is to be a modern central bank that empowers the people of the Solomon Islands. Achieving this vision requires adapting to an increasingly complex operating environment. Transformation efforts focus partly on building leadership

capacity, addressing specific key-person dependencies, ensuring staff possess the required skillsets, strengthening knowledge transfer across the institution, and improving the productivity of CBSI's approximately 170 staff by addressing health-related absenteeism. Another central dimension is digital transformation, ensuring that technological change supports CBSI in fulfilling its mandate in a way that is strategic, forward-looking, and that fosters public trust and financial stability.

- 7. Digital transformation initiatives.** CBSI's digital transformation agenda spans payments infrastructure, financial inclusion, and modernization of internal systems. Key initiatives include the launch of SOLATS, a real-time gross settlement system, in April 2024, with a retail payments module planned as the next step. In 2024, CBSI also partnered with the Solomon Islands National Provident Fund (SINPF) to roll out a digital loan product. In addition, a modernization roadmap for the Bank's IT systems and infrastructure has been developed with support from the US Trade and Development Agency.
- 8. Ongoing IT modernization.** Parallel IT projects are underway to strengthen operational resilience. These include upgrades to the Bank's SWIFT system, establishment of a new data center as part of the headquarters project, rebuilding of production and disaster recovery servers, and advising departments on updating or automating specific manual processes. The ICT Department currently has nine staff, with plans to expand its workforce over the coming year.
- 9. Cybersecurity incident and response.** In May 2024, CBSI experienced a major cybersecurity incident that highlighted the risks inherent in its increasingly complex operating environment. Malware exploiting a zero-day vulnerability linked to staff VPN access compromised multiple systems and network services, with encrypted data preventing the ability to operate many processes. Although backup data and servers were available, the absence of a cyber incident response plan meant that internal systems remained unavailable for up to two weeks. With support from the Australian Government and the private security firm CyberCX, CBSI was able to contain the incident. Since then, the Bank has taken steps to strengthen its resilience by introducing a plan to reduce vulnerabilities, enhancing access controls across systems and applications, and instituting quarterly IT reports to the Management Committee. In addition, CBSI has scheduled regular penetration and backup testing and now runs quarterly staff seminars on phishing, cyber hygiene, and common cyber threats.
- 10. Need for strengthened risk management.** The challenging operating environment and the cyber incident have underscored the need for CBSI to accelerate the maturity of its risk management capabilities. The ERM framework under development consists of ten interconnected components (outlined in Figure 1, with preliminary observations marked in grey). For the framework to operate effectively and support sound, risk-based decision-making, all components must work in harmony and be underpinned by strong and supportive risk leadership.

Figure 1. Risk Management Framework: Observations



Source: Authors.

- 11. Strengthening risk governance at CBSI.** The Central Bank of Solomon Islands (CBSI) has been steadily developing its ERM framework. In 2018, a Risk Management and Corporate Communications Department (RMCCD) was created, with two staff dedicated to risk management. In 2021, the Governor's Office introduced an enterprise-wide incident register template to support systematic reporting of risk events. The following year, the Board Audit Committee's mandate was expanded to include oversight of CBSI's risk management practices, specifically the implementation of the ERM framework, and the committee was renamed the Board Audit and Risk Committee.
- 12. Clarifying the boundary between executive management and board oversight.** In August 2025, the Board approved the expansion of the BARC's membership to include the Deputy Governor. Until then, the Committee had been composed solely of non-executive directors and an independent practitioner from the accounting and audit profession. From a governance standpoint, good practice calls for a clear separation between executive management and oversight functions. To preserve this delineation, the BARC should continue to meet in private session at both the start and end of each meeting, first to consider agenda items and later to reflect on issues raised. The Deputy Governor should therefore not be a formal member of the BARC but could be invited to attend specific discussions in an observer capacity or to participate only during the open portions of the meeting.
- 13. Advancing risk governance through the RMC.** The establishment of the RMC marked an important milestone in strengthening CBSI's risk governance. Chaired by the Deputy Governor, the RMC's terms of reference were approved by the Board in August 2022, and the committee held its first meeting the following month. One of its initial tasks was to draft the Bank's ERMP, which was approved by the Board in late 2023 and formally launched by the Governor in March 2024. The ERMP outlines CBSI's approach to managing risk, defines roles and responsibilities, and introduces a common terminology to ensure risk management is applied consistently to inform decision-making across the organization. At the same time, each department nominated a risk champion to support implementation. Further recognition of CBSI's progress came in

December 2024, when its application for membership of the International Operational Risk Working Group was approved.

- 14. Other risk management developments.** Several risk management initiatives are currently in progress. A revised draft of the ERMP is under review, with a significant addition being a more detailed RAS, which was not included in the original policy. The RMC has also reviewed a draft Business Continuity Management Policy. In parallel, work has advanced on identifying and mapping critical business processes. With support from the USAID TA program for ICT modernization, CBSI completed the mapping of selected critical processes in 2025.
- 15. Remaining gaps in the ERM framework.** Despite recent progress, important elements of CBSI's ERM framework remain incomplete. Departments are not consistently providing basic risk information, only two currently maintain and regularly review risk registers, though such registers are more commonly used for projects. In addition, there is no top-down risk identification process to establish priority risks with a strategic focus. Much of the departmental risk information is gathered through incident reports submitted by risk champions; however, these reports are often focused on low level and less impactful incidents. Clearer expectations are needed regarding both reporting requirements and the role of risk champions. Furthermore, the draft RAS aligns its tolerances with indicators from the Bank's performance management framework, which is designed to monitor strategy execution rather than generate risk insights and assurance.
- 16. Consequences of incomplete risk practices.** The absence of key ERM elements has had significant consequences. Senior leadership lacks a shared and aligned view of CBSI's overall risk profile and its most material risks. As a result, the RMC has been unable to adopt a more strategic role or fully realize the benefits of an effective ERM framework. These gaps have also hindered the development of an integrated risk report. With limited and low-quality risk information, oversight has tended to be narrow, focusing mainly on individual incidents. For example, at its January meeting, the BARC reviewed only the annual summary of incidents and discussed the future implementation of the ERM framework—representing a missed opportunity for deeper challenge and strategic oversight.
- 17. Slow and uneven progress in cultivating the risk culture.** CBSI's risk culture is gradually improving, with risk considerations beginning to feature in some day-to-day departmental discussions. However, progress remains inconsistent across the organization. For example, one department has taken the initiative to compile its own risk register and explore a departmental risk appetite statement, while in other cases management showed limited familiarity with the ERMP and the role of risk champions beyond incident reporting. Inconsistencies in risk reporting were also observed, with some significant incidents omitted while minor issues were recorded. This uneven uptake of the principle that all staff are risk managers is further reflected in delays in approving new risk-related policies and templates.
- 18. Elevating risk oversight in committees.** The quality of risk discussions within oversight committees needs to be strengthened. For the RMC, this means moving beyond summary incident reports and periodic IT updates to a more strategic focus on CBSI's overall risk profile. The committee should review assessments against the Bank's risk appetite and use these insights to inform risk, investment, and policy decisions. Achieving this requires members to be fully engaged in discussions and to adopt an enterprise-wide perspective rather than a departmental one. Oversight could also be improved by streamlining the information provided to the Management Committee and the RMC, given the current overlap. For the BARC, greater emphasis should be placed on risk oversight, rebalancing agendas to allow more time for challenge, monitoring the implementation of outstanding recommendations, and ensuring access to a comprehensive Integrated Risk Report (IRR).

III. Assessment of Previous Recommendations

19. Recommendations for strengthening risk governance. Previous TA reports outlined a structured approach to strengthening risk governance through an ERM framework. They recommended prioritizing the development of the RAS and IRR, supported by an annual governance oversight cycle to ensure continuous refinement and improvement. These steps were seen as essential for moving beyond operational risk management toward a comprehensive, enterprise-wide approach. Once in place, the framework would enable CBSI to adopt a top-down process for identifying strategic risks and enhance the IRR to capture risks that cut across departments. The reports also emphasized the importance of regular staff communication to reinforce risk awareness and culture. Recommendations, commentary, and an updated assessment of progress from the October 2022 TA Report are reproduced in Table 1 below.

Table 1. Recommendations from the October 2022 Report

No.	Recommendation (Priority/timeframe)	Current Status	Comments
			Risk Governance
1.	Establish a Risk Management Committee with appropriate terms of reference (ToR). (High; 3-6 mths)	Complete	The Board approved the RMC's Terms of Reference in August 2022. It met for the first time in September 2022. The Committee mainly comprises Chief Managers from the operational areas and is chaired by the Deputy Governor. It currently meets every two months.
2.	Clearly define the risk management roles and responsibilities. (High; 3-6 mths)	Complete	The Board approved the CBSI Enterprise Risk Management Policy (ERMP) in Dec 2023. The RMP defines risk management roles and responsibilities.
3.	Adopt the Three Lines Model of risk management. (Unassigned)	Partial	The three lines model is defined in the ERMP. Risk Management Unit (RMU) and Internal Audit (IA) are developing charters to clearly articulate their roles and responsibilities.
4.	Include risk oversight within the terms of reference (ToR) for the Board Audit Committee. (Unassigned)	Complete	Risk oversight was included in the revised terms of reference of the Board Audit and Risk Committee in August 2022. Under the ToR the BARC will obtain from RMU a report on implementation of the Bank's ERM framework.
5.	Include risk management (RM)	Partial	Risk incidents are reported to management on a weekly basis

	as a recurring item on the Executive and Board agendas. (Unassigned)		Risk assessments are reported bi-monthly to the RMC and Management Committee (MC). Reporting to the BARC commenced Q1-2025
6.	Ensure a member of each department is assigned responsibility for co-ordinating the risk management process. (High; 3-6 mths)	Partial	Risk Champion (RC) ToRs approved by the Management Committee in February 2024. Department RCs appointed in March 2024. Risk Champions are coordinating incident reports for each department. RMU arranged a tailored risk training workshop for RCs in December 2024. A second training exercise was organized by external facilitators in Fiji in Q1-2025.
7.	Develop a standard risk report for the senior executive and the Board. (High; 3-6 mths)	Partial	A standard risk report is presented to the RMC, MCM and BARC. The report currently focuses on operational incidents and highlights risk areas for executive and senior management discussion.
8.	Management to ensure accurate and timely reporting of risk reporting templates. (High; 3-6 mths)	Complete	Weekly risk incident reporting established in 2021 An incident reporting template and reporting guidelines are currently in use.
9.	Ensure adequate resourcing of Risk Management Unit (RMU). (Unassigned)	Partial	An additional position - Risk and Compliance Analyst - has been earmarked for recruitment in 2025 from the graduate rotation program. Staff in RMU have undertaken training in Power BI. Pending approval of membership with the Risk Management Institute of Australasia (RMIA).
10.	Board Audit Committee to undertake an effectiveness review of its risk oversight. (Unassigned)	Incomplete	This was formalized in the ToR for the BARC in 2022 A risk item is included in the agenda for the quarterly BARC meetings.
			Risk Framework

11.	Formally articulate the CBSI's risk appetite in a Risk Appetite Statement (RAS). (High; 6-12 mths)	Partial	A Risk Appetite framework is incorporated in the latest draft ERMP. The RMC has endorsed a workplan to roll out consultation with the Board, Senior Management and Risk Champions to map risk appetite to the Bank's risk register. A phased project over 6 – 8 months is envisaged with a deadline of Q1-2026.
12.	Engage departmental risk experts to define appropriate risk thresholds (tolerances). (High; 6-12 mths)	Incomplete	This task is expected to be undertaken in Q4-2025. It should be part of the Bank's RAS.
13.	Establish the methodology for risk identification (bottom up and top down) and risk assessment to be endorsed by the RMC. (High; 6-12 mths)	Partial	The bottom-up risk identification methodology is incorporated in the revised ERMP. While departmental Risk Registers will be the main tool for the bottom-up approach, currently only two departments complete departmental risk registers. There is some awareness of the concept as risk registers are used for larger projects. The current draft ERMP says little about implementing the top-down approach to identifying Key Enterprise Risks.
14.	Align leadership on the frequency of the Strategic Risk Assessment (SRA) (Unassigned).	Incomplete	This is under review as part of the introduction of the Bank's performance management framework.
15.	RMC to ensure senior management alignment on risk materiality. (High; 6-12 mths)	Partial	Current alignment on risk materiality is through the escalation of incident reports to senior management. The RMC escalates unresolved incidents to the Management Committee for discussion.
16.	Cultivate risk leadership at all levels (Unassigned)	Partial	There is some risk leadership at the RMC, MC and BARC committees. There is limited departmental risk leadership owing to competing demands on senior management, who are currently focused on other key institutional initiatives. This has limited their capacity to provide active risk leadership.

17.	Calibrate integrated risk reporting to reflect the structure of the RAS. (High; 6-12 mths)	Incomplete	Revised ERMP provides some clarity for future risk reporting as it will reflect the structure of the Risk Appetite Statement (RAS).
18.	Formalize the governance and procedures for incident management. (Unassigned)	Complete	Governance and procedures for the reporting of incidents have been established. Summary reports are being made available to the RMC, MC and BARC.
19.	Provide the Board, leadership and staff with ongoing risk seminars and training. (Unassigned)	Partial	Board members and Executive received Risk Governance training from the Governance Institute of Australia in Q1-2025. RCs, Senior Management and the Chair of the BARC participated in risk management training in December 2024. RCs and Senior Management attended risk management training in February 2025 Refresher training will be rolled out following the approval of the revised ERMP.
			Business Continuity Management
20.	Formalize the governance and procedures for business continuity management (BCM). (Unassigned)	Partial	A BCM policy has been drafted and reviewed by the RMC. Approval is pending input from the senior management team.
21.	Create a critical Incident Management Team (IMT). (Unassigned)	Partial	An Incident Response Taskforce is part of the draft BCMP but its composition varies and its responsibilities are only defined at a very high level as 'first responders'. The Taskforce is likely to comprise key senior management from operational departments including ICT, HRCSD, FAD, CBSD, RMCCD. As currently drafted, this team is headed by the Governor.

			Other
22.	Engage with peers and IORWG on risk management. (Unassigned)	Complete	CBSI granted membership of the IORWG in Q4-2024 RMU now participates in IORWG benchmarking surveys. It will send a participant to the IORWG conference scheduled for Q3-2025.

20. Key milestones achieved in risk management. Several important tasks have already been completed in strengthening CBSI's risk governance. These include establishing the RMC, revising the BARC's terms of reference to incorporate oversight of risk management, and defining risk management roles and responsibilities in line with the Three Lines Model. In addition, CBSI has introduced an incident and near-miss reporting framework and, in December 2024, secured membership in the International Operational Risk Working Group.

21. Progress achieved, but significant work ahead. Since the last onsite mission, CBSI has made progress in strengthening its risk management framework, though further work remains. In terms of the assessment table, progress has improved from red to yellow. Key developments include:

- Integrated Risk Reporting: One component of the IRR, the incident report, is now produced for both the Management Committee and the RMC. In March 2025, the RMU Manager also presented an annual incident review and an outline of the proposed IRR to the BARC. The planned IRR will include a risk appetite compliance assessment, CBSI's most material risks, key risk indicators, and updates on risk assessments and risk mitigation activities.
- Risk Appetite: The latest draft of the ERMP now includes a RAS covering 23 categories of risk, an enhancement over the limited scope of the version approved in December 2023. An appendix sets out tolerances for key risk indicators in selected categories, though these require further development to provide sufficient assurance.
- Risk Identification: The ERMP incorporates standardized risk rating matrices and detailed coverage of risk identification. However, there is still no formal top-down process for identifying strategic risks. At the departmental level, only two units maintain and regularly review risk registers. To help address this, the RMU has prepared a template and guidance materials, which are pending approval.
- Business Continuity Management: A draft Business Continuity Management Policy is under active review by the RMC, alongside the proposed establishment of an incident response taskforce as part of the plan.
- This progress has been supported by improved resourcing. The RMU is now fully staffed with a manager and two analysts (risk and compliance, and middle office), following it being under staff complement due to extended study leave.

22. Areas of slow progress and future priorities. In several areas, progress has been limited, and the TA mission's assessment remains unchanged from the previous review. These include that priorities include embedding the Three Lines Model, improving the effectiveness of the BARC and RMC, alignment on risk materiality, and cultivating the risk champion network. The August 2024 TA Report, summarized in Table 2, reaffirmed that the original recommendations and priorities for strengthening risk management remain highly relevant. The additional recommendations

provided were intended to guide and support the implementation of those priorities, with an increased emphasis on business continuity.

Table 2. Recommendations from the August 2024 Report

	Recommendation (Priority; timeframe)	Current Status	Comments
			Risk Governance
A.	The Board Audit & Risk Committee (BARC) should re-weight its agenda. (High; (Q2-2024))	Partial	The BARC has a risk item on its agenda. The discussion currently relates to incidents. At its meeting in January 2025 the Manager, RMU, presented on incidents, RMU's role, what an integrated risk report might look like and some future milestones for adopting an ERM framework. initiative. There was no discussion of risk at the May 2025 meeting.
B.	RMU should develop an integrated risk report (IRR). (High; (Q2-2024))	Partial	Current risk reporting is confined to incidents. The desired components of an IRR was presented to the BARC in January 2025. It included items such as reporting against risk appetite, the Bank's risk profile, risk insights, risk metrics and key risk indicators and regulatory and compliance updates.
C.	RMU should focus on the development of the Risk Appetite Statement (RAS). ((High; (Q2-2024))	Partial	The revised RMP incorporates a Risk Appetite Statement (RAS). Risk thresholds are currently based on indicators in the Bank's Performance Management Framework. Some of these are very subjective. To progress, there will need to be discussions with various internal stakeholders, including departmental management, the Board, Executive and Senior Management, Risk Champions and the general staff. This phase of the project is scheduled to commence in Q4-2025
D.	Reduce the frequency of meetings of the RMC from monthly to bi-monthly. ((Low; (Q2-2024))	Complete	The RMC has been meeting every two months since Sept 2023
			Embedding the Three Lines of Defense Model

E.	Strengthen the tone from the top. <i>((Medium; (Q2-2024))</i>	Complete	The ERM framework was launched by the Governors in March 2024. The rollout, which involved all staff, was designed to demonstrate commitment to the introduction of ERM at the CBSI. Since then, training and awareness programs have been undertaken targeting risk management personnel, risk champions and other staff more broadly.
F.	Provide enhanced risk insights. <i>((Medium; (Q2-2024))</i>	Partial	The incident register is the primary source of information that is reported to RMC, MCM and the BARC and used to generate insights. The Report also provides updates on unresolved incidents
			Business Continuity Management/Critical Incident Management
G.	Further enhance the governance of BCM. <i>((High; (Q4-2024))</i>	Partial	A draft Business Continuity Management Policy was presented to the RMC for first comments in Q2-2025. A second round of comments from the RMC and final Board approval is expected by the end of Q3-2025.
H.	Facilitate a structured business continuity response. <i>((Medium; (Q2-2024))</i>	Partial	An Incident Response Taskforce has been identified in the draft BCMP. Its composition, which depends on the nature of the incident, would draw from the Governors, Advisors and senior management team in operational departments. Its role is defined as a 'first responder' to an incident.
I.	Improve the BCM process. <i>((Medium; (Q5-2024))</i>	Partial	CBSI completed a business process mapping of certain critical processes in 2025, with support from the USAID Technical Assistance (TA) program for ICT modernization. The output from this initiative will underpin the Business Impact Assessment (BIA). Preliminary discussions have been held with departments on the design and structure of a standardized BIA template to ensure consistent identification of critical processes, dependencies, and alternate arrangements during disruptions.

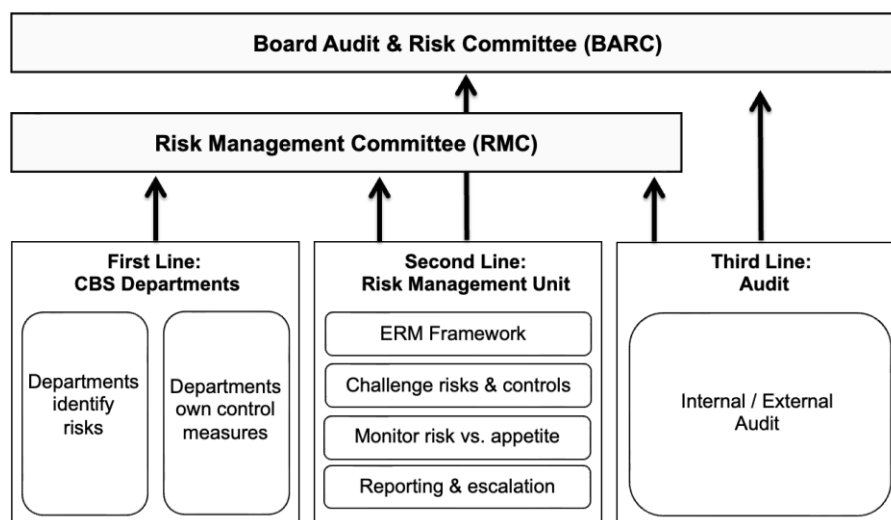
23. Progress achieved, but critical priorities still lagging. The overlap between the two TA reports means that the assessments of recommendations in the second report are broadly consistent with those in the first. One completed recommendation was to reduce the frequency of RMC meetings from monthly to bi-monthly, a change that the RMU reports has improved productivity by freeing up time to implement the framework. While progress has been made in several areas, it remains slow and has not kept pace with suggested timeframes. More importantly, momentum has not been focused on the highest-priority initiatives—particularly the development of a comprehensive Risk Appetite Statement (including risk tolerances), improved risk identification processes, and the completion of the IRR. Although resourcing issues have been partly resolved, stronger prioritization will be needed to ensure these critical elements are delivered.

IV. Other Observations

A. Implementation of the Three Lines Model of Risk Management

24. Governance alignment with the Three Lines Model. CBSI's governance framework is aligned with the TLM of risk management, as shown in Figure 2. The TLM's main strength lies in the clarity it brings to governance, with well-defined roles and responsibilities that reduce duplication, confusion, and accountability gaps. To fully realize its benefits, such as stronger risk awareness, better decision-making, and more effective oversight, each line must take full ownership of its responsibilities and actively carry them out.

Figure 2. The Three Lines Model of Risk Management



Source: Authors.

25. Enhancing BARC's risk oversight role. The BARC agenda should deliver consistent and proportionate oversight of risk management, with sufficient time dedicated to risk at every meeting. Key priorities include monitoring the implementation of outstanding ERM recommendations, providing informed challenge on risk issues, and proactively engaging with staff to ensure the Board and BARC are assured that priority risks are being identified, assessed, and effectively managed. Information should flow in both directions, through departmental

submissions and constructive challenge from the RMU, and with oversight by the RMC and the BARC helping to guide and shape the structure and content of the IRR.

26. **Membership of the BARC.** The BARC plays a vital role in providing independent oversight of financial reporting, internal controls, risk management, and the work of the internal and external auditors. Its effectiveness depends on the independence, both actual and perceived, of its members from day-to-day management. In line with international best practice, including the Basel Core Principles and OECD governance guidelines, many central banks explicitly exclude executives from audit committee membership to safeguard the integrity of oversight. While executives may attend specific sessions by invitation, for example, to present reports or respond to questions, they do so without voting rights and on a limited basis. Given the Deputy Governor's operational and strategic responsibilities, their membership on the BARC could therefore create a perceived or actual conflict of interest and risk undermining the committee's objectivity and independence.
27. **Keeping the RMC strategic and disciplined.** The RMC plays a central role in coordinating and overseeing CBSI's ERM framework, particularly in its early stages, to ensure the Three Lines Model functions cohesively across the organization. While the committee already follows a structured agenda, it must remain disciplined in prioritizing its work to avoid becoming overly administrative. Near-term priorities include overseeing the setting of risk tolerances within the RAS, identifying the Bank's priority risks, and advancing development of the IRR. The RMC can also strengthen first-line accountability by inviting departments to present their risk profiles. Ultimately, its discussions should move beyond operational details to a more strategic focus on risk insights.
28. **Clarifying the Chief Risk Officer role.** To strengthen accountability, CBSI should clarify who is responsible for performing the Chief Risk Officer (CRO) function. The CRO is critical to ensuring the Three Lines Model operates as an integrated, strategic system rather than a collection of separate roles. While responsibilities are distributed across the three lines, the CRO provides organization-wide coordination and leadership of risk efforts. Currently, it is unclear who is driving CBSI's risk agenda with the necessary authority and sponsorship. One option is for the Deputy Governor to assume this role, given the position's responsibility as RMC chair, its ability to mobilize resources, and its influence in fostering a stronger risk-aware culture.
29. **Strengthening communication between the second and third lines.** Effective communication between the RMU (second line) and Internal Audit (third line) at the CBSI is critical to avoiding duplication and ensuring coordinated oversight. Timely information-sharing will allow the second line to provide insights on emerging risks, controls, and compliance issues, while the third line can use this intelligence to refine audit priorities and focus on the areas of greatest concern. Strong alignment between the two functions will enable earlier detection of systemic weaknesses, more effective corrective actions, and promote transparency and continuous improvement. Together, this will ensure that the Board receives a cohesive and comprehensive view of risk and control effectiveness. The Second line has responsibility for the design and operation of the framework, while the Third Line is responsible for providing independent assurance that the ERM framework is operating effectively.

B. Risk Appetite

30. **Risk appetite as the foundation of ERM.** A clearly articulated risk appetite and set of risk tolerances are fundamental to a strong ERM framework. Risk appetite defines the types and levels of risk an organization is prepared to accept in pursuit of its objectives. It ensures that

strategic goals are pursued within acceptable boundaries, preventing both overreach and excessive caution. It also supports leadership in making consistent, aligned decisions that reflect the organization's mission and values.

- 31. Current ERMP coverage of risk appetite.** The current ERMP provides only limited coverage of risk appetite. However, the latest draft introduces a RAS that addresses 23 risk categories. For each category, the draft describes the risk, nominates a risk appetite, and identifies a risk owner. It also assigns responsibility for certain risks to specific Bank committees, for example, monetary policy risks to the Monetary Policy Committee, and risks linked to the supervision of financial institutions to the Financial Stability Committee.
- 32. Developing risk tolerances for effective oversight.** Risk tolerances translate the high-level concept of risk appetite into practical thresholds that guide day-to-day operations. They set acceptable levels of variation around objectives, enabling teams to recognize when a risk is within limits or when escalation is required. By bridging strategy and execution, they make risk appetite meaningful to first-line owners. The current draft includes tolerances for selected key risk indicators across a subset of categories, but these require further development. Effective risk tolerances should be quantifiable, objective, forward-looking, integrated into regular risk reporting, and subject to periodic review.
- 33. Identifying potential metrics for risk tolerances.** The discussion with the CBSI team highlighted several areas that could serve as a foundation for developing risk tolerances. These include:
- Data from the vulnerability assessment performed by CyberCX following the ransomware attack in 2024;
 - Staff participation in cyber awareness training;
 - A business continuity recovery time objective specifying how quickly CBSI can transition from primary to backup servers, validated through scheduled tests (e.g., every six months); and
 - Import coverage in months for foreign exchange reserves.
- 34. Embedding risk tolerances across the CBSI.** Discussions on risk tolerances should begin with departmental management before being reviewed at all levels of the organization. Risk tolerances are essential, as they provide the basis for assessing whether CBSI is operating within its risk appetite for each risk category—an assessment that feeds directly into the Integrated Risk Report. To finalize risk tolerances efficiently, departmental engagement will require strong support from the RMC. In addition, an annual review of their appropriateness should be built into the Bank's governance timetables.

C. Risk Identification

- 36. Strengthening risk identification through a combined approach.** CBSI has been slow to define its risk profile and to align stakeholders on its priority risks, largely because only a few departments are compiling risk registers and there is no structured process for identifying strategic risks. A top-down approach to risk identification, led by senior executives and focused on strategic risks aligned with organizational goals, has not yet been instituted. When combined with a bottom-up process, which captures risks arising from daily operations, this approach creates a more resilient and adaptable organization while helping to surface blind spots, such as shared responsibilities for business continuity. Implementing a top-down approach requires

structured engagement with senior leaders, using open-ended discussions to uncover emerging concerns and organizational vulnerabilities. Cross-functional workshops can then be used to explore interdependencies and ensure risks are assessed comprehensively.

- 37. Standardizing bottom-up risk identification.** For bottom-up risk identification, the RMC should ensure that all departments complete risk registers using a standard template provided by the RMU. These registers should be reviewed regularly, such as after an incident, or at least annually as part of a scheduled cycle. To keep the process efficient, the template should be streamlined, supported by clear guidance, and focused on priority risks (for example, departments could be asked to nominate no more than 10). The RMU might also specify a set of common risks (e.g., fraud) that every department assesses, enabling organization-wide mapping. Providing structured guidance on how to frame risk statements—*an event* (), *caused by* (), *with consequences for CBSI* ()—would help ensure risks are described clearly and consistently.
- 38. Managing increased risk data and tools.** CBSI will need to determine how the RMU manages the larger volume of information generated through risk identification. At a minimum, this requires adopting standardized templates (primarily in Excel) and equipping staff with data analytics tools. CBSI has already begun training some staff, including those in the RMU, to use Microsoft Power BI for data aggregation. It is also considering the purchase of an off-the-shelf risk management system. However, the TA mission advises deferring such a decision until the ERM framework is more firmly embedded, when CBSI will be better positioned to assess and select the most suitable option.

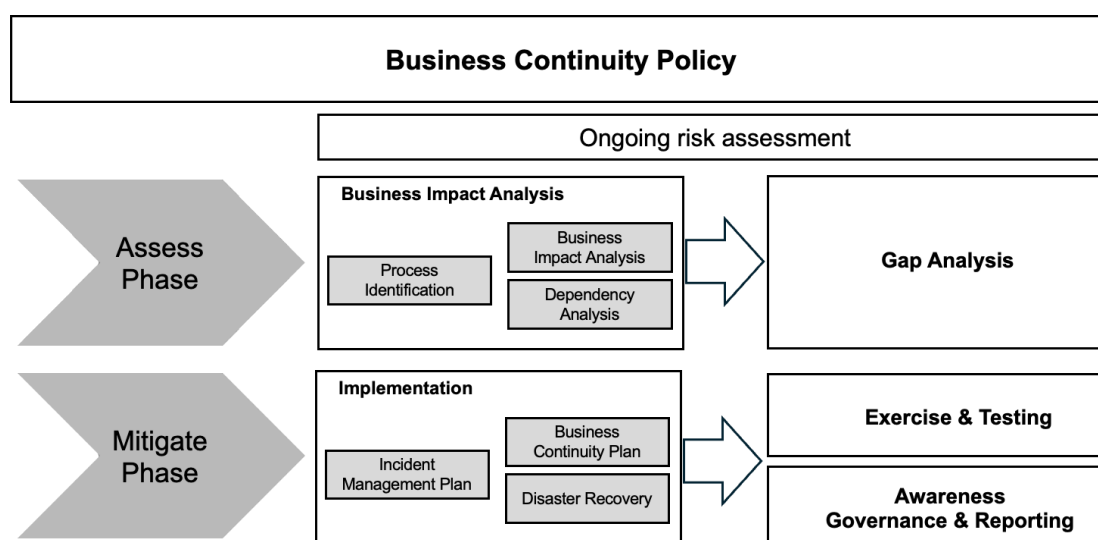
D. Incident Reporting

- 39. Clarifying the role of incident reporting.** The introduction of the incident reporting regime has raised risk awareness at CBSI, but some confusion remains. Staff are unclear about the distinction between a risk register and an incident register, and not all incidents, particularly serious events or material near misses, are being reported. At the same time, some reports capture business-as-usual issues more suited to facilities or IT help desks. Additional guidance is also needed on how to manage sensitive incidents, such as those received through a whistleblower hotline. A further concern is the perception that the RMU plays a policing role, creating uncertainty about the purpose of reporting and the role of risk champions.
- 40. Purpose of incident and near-miss reporting.** The incident and near-miss reporting regime is designed to act as a real-time feedback loop that strengthens risk awareness, resilience, and continuous improvement. Near misses often serve as early warnings of more serious events, while actual incidents can reveal risks not captured in registers. Analyzing why incidents occur helps prevent recurrence, reinforces a culture of open reporting without fear, and highlights systemic weaknesses through data patterns. Each reported event, whether an incident or near miss, represents an opportunity to refine CBSI's processes and strengthen organizational resilience.
- 41. Updating guidance to strengthen reporting.** There is a clear case for updating guidance on incident and near-miss reporting. Revised guidance should explain why the RMC values this information, how incident registers connect to risk registers, and the importance of capturing all unplanned events that result in—or have the potential to result in—harm, damage, or loss to CBSI. While this definition would normally exclude minor business-as-usual events, special arrangements may be required for a narrow set of highly sensitive cases. Otherwise, all incidents and near misses should be recorded. The RMC's discussion of incidents should also move beyond case-by-case reviews to focus on generating broader risk insights.

E. Business Continuity

- 42. Renewed focus on business continuity.** CBSI has placed greater emphasis on business continuity following the May 2024 ransomware attack and the evolving risk landscape. A draft Business Continuity Management Plan (BCMP) has been prepared and reviewed by the RMC. The plan outlines its objectives, examples of continuity events (primarily natural disasters and operational incidents), a planning framework using business impact assessments, the formation of an incident response task force, guidance on committee and taskforce roles, and requirements for testing and reporting.
- 43. Clarifying governance roles in BCM.** The draft BCMP would benefit from clearer articulation of governance roles. In most central banks, the RMC, supported by the RMU, provides executive oversight of BCM but not its direct implementation. The RMC ensures alignment on critical processes, sets recovery time objectives in consultation with departments, and oversees incident simulations through the Critical Incident Management team. Progress is normally reported through the IRR. The RMU could coordinate BCM, though additional resources would be needed to avoid undermining its broader second-line responsibilities. Implementation of the plan is typically assigned to a specific department, most often corporate services or IT (for IT disaster recovery).
- 44. Establishing a structured business continuity framework.** The Business Continuity Management Plan (BCMP) should articulate a clear and structured approach to continuity management. As illustrated in Figure 3, an effective framework includes: (i) identifying critical processes through a Business Impact Analysis (BIA), with a standard template provided by the RMU, building on work already completed under the USAID IT modernization program; (ii) conducting risk assessments to evaluate the likelihood and impact of foreseeable internal and external threats; (iii) developing and documenting continuity plans, informed by the BIA and risk assessment, and implementing risk mitigation measures; (iv) conducting training, exercises, and testing; and (v) ensuring ongoing monitoring, updating, and reporting. To remain effective, the plan should be kept simple and flexible.

Figure 3. Business Continuity Management



Source: Authors.

- 45. Incident management team as the core of BCM.** A central feature of most Business Continuity Management Plans (BCMPs) is the establishment of an Incident Management Team (IMT) to coordinate rapid and effective responses to disruptions. The IMT should have clearly defined roles and responsibilities, criteria for activation, pre-established communication channels, and regular drills to test readiness. Its operations should align with IT recovery timelines and resource allocations. The team is typically led by a senior staff member, though not necessarily the Governor, who has the authority to mobilize resources quickly. Membership may be expanded depending on the nature of the incident. Following resolution, the IMT conducts a post-incident review to capture lessons learned and strengthen future responses.
- 46. Testing as a driver of credibility and resilience.** Testing and learning from both internal experiences and external events are essential elements of BCM. Testing must be realistic and reflect the Bank's risk environment: while natural disasters pose a high probability of disruption in Solomon Islands, reputational risks are more acute when the source of disruption is CBSI itself. This distinction should guide the scope and schedule of testing activities. Demonstrating the ability to respond effectively to disruptions enhances the Bank's credibility and resilience, particularly in the eyes of the institutions it interacts with and supervises.

V. Next Steps

- 47. The figure below gives some idea of how these tasks might be prioritized over the next year and a half.**

Figure 4. Actions

Action	Timeline
Risk Governance	
Review BARC membership to ensure clear separation between executive management and board oversight	Q1 2026
Re-weight Board Audit & Risk Committee agendas to allow sufficient time for oversight of the risk profile	Q1-2026
Elevate dialogue at the RMC to foster a more strategic review of risk and incident insights	Q1-2026
Focus RMU on coordinating risk tolerances, to finalize RAS, and prepare first Integrated Risk Report (IRR)	Q1-2026
Embedding the Three Lines Model	
Tone from top: Increase frequency of communications to promote a culture of "all staff are risk managers"	Q2-2026
Build on initial departmental risk incidents, with RMU to focus on completing quality assurance and to translate risk and incident information to insights for RMC and BARC in IRR	Q2-2026
Business Continuity Management / Critical Incident Management	
Evaluate and implement and resource chosen option to establish CBSI-wide BCM coordination capability	Q2-2026
Develop and implement Business Impact Assessment (BIA) to identify critical processes	Q3-2026
Integrate governance of BCM to RMC and Board Audit & Risk Committee	Q4-2026

- 48. BARC's role in driving risk oversight.** BARC must dedicate focused time at each meeting to risk discussions, with initial attention on progress in implementing ERM at CBSI. This includes reviewing business continuity arrangements and remedial actions following the May 2024 ransomware attack. To gain sufficient assurance over CBSI's risk management practices, BARC should provide robust challenge to the material presented and ensure clear accountability for follow-up actions. A resource that may be of some assistance to the BARC (and executives) is the IMF Working Paper entitled *Risk Management Maturity at Central Banks* (WP/19/303).

- 49. RMC priorities for strengthening risk governance.** The RMC has several priorities: aligning stakeholders on CBSI's highest priority risks (supported by departmental risk profile presentations), approving the RAS and risk tolerances, and elevating meeting discussions from operational detail to strategic insights. The RMC must also decide how to resource BCM and integrate its governance into the committee's remit. Greater communication from leadership reinforcing that all staff are risk managers would strengthen accountability. In addition, the RMC should clarify who is responsible for fulfilling the Chief Risk Officer function, so that the responsible lead for driving the design and implementation of the framework is clear.
- 50. RMU's role in building risk tolerances and insights.** The RMU's priority is to develop risk tolerances for each sub-category in the RAS, in consultation with departments, the Board, and the RMC. It must also provide templates and guidance for departmental risk registers. A continuing responsibility is to generate insights from departmental inputs and communicate these to the RMC, Board, and BARC. As these tasks progress, the RMU will be able to gradually build out the IRR.
- 51. Departmental responsibilities in risk management.** Departments must complete risk registers using the RMU's standard template, reviewing them after incidents or at least annually. All incidents should be included in these registers. Departments also have a key role in business continuity by identifying and mapping critical business processes. This will allow BIAs to be carried out, identifying the positions and systems most critical to CBSI operations.
- 52. Follow-up support and Board engagement:** It is recommended that CBSI schedule a short follow-up TA mission within 18–24 months, culminating in a risk management seminar and workshop for the Executive and Board. The workshop should provide an opportunity to assess progress in embedding the ERM framework, review lessons learned from incident reporting and business continuity testing, and evaluate the effectiveness of the RAS, risk tolerances, and IRR. Additional content could include case studies from peer central banks, scenario-based exercises to strengthen strategic risk identification, and a dedicated session on the evolving role of the Board in risk oversight. This follow-up will help ensure sustained momentum, reinforce accountability, and strengthen CBSI's overall risk culture.

VI. Concluding Remarks

- 53. Strengthening risk governance and oversight.** Robust risk governance is essential for protecting CBSI's reputation, credibility, and operational independence. Clear governance structures enhance accountability and transparency, and the Three Lines Model provides an effective framework by delineating roles and responsibilities to support sound risk management. Successful implementation, however, requires a well-defined separation between executive management and Board oversight, as well as broad institutional understanding and execution of assigned responsibilities. Strong leadership from the RMC and BARC is particularly important during the initial implementation phase, as their sustained engagement will help build momentum and institutionalize good practice.
- 54. Building a supportive risk culture.** A strong risk culture is the glue that holds the ERM framework together and amplifies its effectiveness. While there are encouraging signs, such as departments showing greater engagement with the framework, there are also weaknesses, including limited review and challenge, reluctance to report incidents, siloed first line practices, and a lack of strategic appreciation for how ERM strengthens the organization. Addressing these cultural gaps is essential to embedding risk management as a shared responsibility.

- 55. Maintaining momentum at a critical junction.** CBSI is at a pivotal stage, with several important initiatives well advanced but not yet approved, including the revised ERMP, the departmental risk register template, and the business continuity management policy. Advancing these initiatives requires clear organizational priorities, defined accountability, and visible support from senior leadership and the Board. Business continuity offers a key test of CBSI's readiness: disruptions are inevitable in a complex, digital environment, but what matters is the Bank's ability to minimize their impact on both CBSI and the wider Solomon Islands community. CBSI's credibility will depend on demonstrating that it has learned from past experiences and can respond effectively.
- 56. Follow-up TA and Board workshop.** A follow-up TA mission is recommended within 18–24 months, incorporating an Executive and Board workshop to assess progress in embedding the ERM framework. This will help sustain momentum, enhance accountability, and reinforce a risk-aware culture across the organization.

Appendix I. List of People Met

Board

Helen Beck Member, Chair of the Board Audit and Risk Committee

Board Audit and Risk Committee

Joshua Tuasulia Independent Member of the Board Audit and Risk Committee

Senior Leadership

Luke Forau	Governor
Raynold Moveni	Deputy Governor
Richard Muaki	Chief Fiduciary Officer
Marlon Houkarawa	Management Advisor, Operations
Michael Kikiolo	Management Advisor, Policy

Management

Sonia Marahare	Chief Manager, RMCCD
Charley Kuper	Manager Risk, RMCCD
Lynne Suti	Risk and Compliance Analyst, RMCCD
Edward Manedika	Chief Manager, ICTD
Glen Buka	Chief Information System Officer, ICTD
Knoxly Otto	IT Operations & Support Analyst, ICTD
Errol Kausimae	Senior Systems and Network Analyst, ICTD
John Rohi	Manager Financial Markets, FMECD
Charlie Sivukana	Manager Exchange Control, FMECD
Joe Vasuni	Chief Manager, CBSD
Enoch Ilisia	Manager, CBSD
John Bosco	Chief Manager, HRCSD
Michael Erekal	Manager, Corporate Services, HRCSD
Jenny Inimae	Manager, Human Resources, HRCSD
Simon I'io	Supervisor, Properties, HRCSD
Emmanuel Gela	Chief Manager, FAD
Simon Ramoifai	Manager, FAD
Sandy Iro	Chief Manager, ERSD
Ronsly Pana	Manager, ERSD
Daniel Haridi	Chief Manager, FSDPD
Linda Folia	Manager, Financial Inclusion, FSDPD
Samuel Warunima	Chief Manager, FSRD
Denson Denni	Manager—Applied Research Policy & Regulation, FSRD
Mary Loea	Manager—Financial Institutions Supervision, FSRD
Millisidy Pita	Senior Analyst—Superannuation and Credit Institution, FSRD
Eddie Maek	Senior Insurance Analyst, FSRD
Ellen Masa	Analyst, FSRD

Frederick Maina	Senior Banking Analyst, FSRD
Janice Jun Leziton	Credit Union Analyst, FSRD
Jared Fagasi	Analyst, FSRD
Norman Vavaha	Senior Credit Union Analyst, FSRD
Steeve R. Awao	Senior Research & Policy Analyst, FSRD
Jimmy Vaja	Manager, Intelligence Management, FIU
Kevin Murray	Assistant Manager, IA
Oliver Karoa	Manager, IA

Appendix II. Schedule of Meetings

#	Session	Date	Duration (hours)
1	Risk Management & Corporate Communications Department	July 21, 2025	1
2	Governor and Deputy Governor	July 21, 2025	1
3	Internal Audit	July 21, 2025	0.75
4	Information Communication Technology Department	July 22, 2025	1
5	Financial Markets & Exchange Control Department	July 22, 2025	1
6	Currency and Banking Services Department	July 22, 2025	1
7	Finance & Accounts Department	July 22, 2025	0.75
8	Economics, Research & Statistics Department	July 22, 2025	0.75
9	Risk Management Committee	July 23, 2025	1.0
10	Board Audit and Risk Committee	July 23, 2025	0.75
11	Risk Champions	July 23, 2025	0.75
12	Financial System Regulation Department	July 23, 2025	1
13	Human Resources & Corporate Services Department	July 23, 2025	1
14	Financial Systems Development & Payments Department	July 23, 2025	1
15	Presentation to Board and Senior Leaders of Preliminary Findings	July 24, 2025	1.5
16	Risk Management Unit Workshop	July 25, 2025	2

Appendix III. Documents Reviewed or Consulted by the Mission

In addition to the artefacts made available to the Mission for its previous report the following documents were reviewed or consulted by the mission team.

#	Document Title	Date of Issue
1	Enterprise Risk Management Policy	December 2023
2	Enterprise Risk Management Policy (draft) – includes Risk Appetite Statement	March 2025
3	Risk Management Committee Terms of Reference	August 2022
4	Board Audit and Risk Committee Terms of Reference	August 2022
5	Risk Management Committee meeting agendas	January, May 2025
6	Incident Reporting Form	
7	Incident Management Policy (draft)	
8	Business Continuity Management Policy (draft)	July 2025
9	Incident Report Monthly Summary	
10	Consolidated Risk Incident Report Annual Summary	2024
11	Risk Champions Terms of Reference	February 2024
12	CBSI Annual Report	2024

Appendix IV. Virtual Follow-ups

#	Date	Topics Discussed
1	Apr. 24	RMU Manager in place after study leave absence; Risk Management Policy approved; RMU updates to BARC; risk appetite statement
2	Jul. 24	Risk appetite statement and Key Risk Indicators; risk taxonomy
3	Oct 24	Risk workshop; Risk Management Committee operations; risk appetite statement; incident management; risk registers; peer engagement
4	Feb. 25	Risk management workshop; risk champions; incident reporting; risk appetite; departmental risk registers; performance management framework
5	May 25	RMU staff rotation; risk appetite framework; performance management framework