



# TECHNICAL ASSISTANCE REPORT

## **SRI LANKA**

Central Bank Risk Management

**SEPTEMBER 2024**

**Prepared By**

*Gabriel Andrade and Mariam Manjgaladze (MCM External Experts)*

**Authoring Department:**

**Monetary and Capital Markets  
Department**

## **DISCLAIMER**

---

*The contents of this report constitute technical advice provided by the staff of the International Monetary Fund (IMF) to the authorities of Sri Lanka in response to their request for technical assistance. This report (in whole or in part) or summaries thereof may be disclosed by the IMF to the IMF Executive Director of Sri Lanka, 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 interest unless the CD recipient specifically objects to such disclosure (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 MCM Department.*

Contents	Page
Glossary.....	4
Preface.....	5
Executive Summary .....	6
I. Introduction.....	9
II. Risk Management Governance.....	9
A. Current Situation .....	9
B. Recommendations.....	11
III. Risk Management Framework and Appetite.....	13
A. Current Situation .....	13
B. Recommendations.....	16
IV. Strengthening the Three Lines Model.....	17
A. Current Situation .....	17
B. Recommendations.....	19
Tables	
1. Key Recommendations.....	7
Figures	
1. Risk Management and Governance Structure of the CBSL.....	11
2. Strategic Risk Management .....	12
3. Risk Taxonomy of the CBSL.....	15
4. Key Risk Indicators.....	16
Appendices	
I. List of the Documents Shared with the Mission.....	21
II. List of People Met .....	22
III. Organizational Chart of the CBSL.....	23
IV. Boards of the NBSL.....	24
V. Risk Committees of the NBSL.....	25
VI. Presentation from the Mission .....	26

## GLOSSARY

AC	Audit Committee
AG	Assistant-Governor
BCP	Business Continuity Planning
BROC	Board Risk Oversight Committee
CBSL	Central Bank of Sri Lanka
CBRM	Central Bank Risk Managers
CCO	Chief Compliance Officer
CISO	Chief Information Security Officer
CRO	Chief Risk Officer
DG	Deputy Governor
DRO	Departmental Risk Officer
GB	Governing Board
HR	Human Recourses
IA	Internal Audit
IAD	Internal Audit Department
IFIs	International Financial Institutions
IMF	International Monetary Fund
IORWG	International Operational Risk Working Group
IT	Information Technology
KRI	Key Risk Indicators
MB	Monetary Board <sup>1</sup>
MCM	IMF Monetary and Capital Markets Department
MPB	Monetary Policy Board
NFRMC	Non-Financial Risk Management Committee
ORMG	Operational Risk Management Guidelines
RAF	Risk Appetite Framework
RAS	Risk Appetite Statement
RCO	Risk Coordinating Officers
RCSA	Risk and Control Self-Assessment
RMD	Risk Management Department
RMPS	Risk Management Policy Statement
SDG	Senior Deputy Governor
SRA	Strategic Risk Assessment
TA	Technical Assistance

---

<sup>1</sup> With the new Central Bank Act enacted on 15.09.2023 the Monetary Board ceased to exist and the Governing Board and the Monetary Policy Board came to existence.

## PREFACE

At the request of the Central Bank of Sri Lanka (CBSL), a Monetary and Capital Markets Department (MCM) hybrid technical assistance (TA) mission took place in Q4 2023. Virtual interactions were conducted during October and November 2023; the onsite mission took place in Colombo from November 27 to December 4, 2023. The mission comprised Mr. Gabriel Andrade and Ms. Mariam Manjgaladze (MCM experts, respectively from the Bank of Portugal and the National Bank of Georgia). The mission was backstopped by Mr. Ashraf Khan at IMF HQ. Appendix I lists the documents consulted and reviewed by the mission.

The purpose of the mission was to assist the CBSL in further improving its risk management, contributing to more effective and efficient central bank decision-making, thereby helping the CBSL to work towards achieving its (legal) mandate. Financial risk management was out of the scope for this TA mission but the team took note of the recent IMF TA on financial risk management - Strengthening the Risk Assessment of the Central Bank of Sri Lanka (November 2023).

The mission had helpful and in-depth discussions with Governor Dr. P. Nandalal Weerasinghe, Senior Deputy Governor (SDG) Mrs. T. M. J. Y. P. Fernando, Deputy Governor (DG) Mrs. K. M. A. N. Daulagala, Board Risk Oversight Committee (BROC) Independent External Members Mr. H. A. Karunaratne and Mr. Trevine Jayasekara, and several Assistant-Governors (AGs)/Directors of CBSL departments. Extensive in-depth sessions focused on sharing information, advice, and insights into best practices were conducted by the TA mission with the Head of Risk Management Department (i.e. Chief Risk Officer (CRO)) Mr. W. R. M. K. Fernando and the full RMD team. Additionally, a dedicated 2-hour meeting/awareness session was organized with all Directors/RCOs, facilitated by the mission. Appendix II lists the stakeholders with whom the mission team met. Appendix VI contains the slides presented by the mission during its closing meeting.

The mission wishes to thank all CBSL colleagues for their cooperation, productive discussions, and hospitality. In particular, the mission would also like to thank Mrs. Thilini Jayasinghe, Senior Assistant Director of RMD, for her continued support in facilitating the mission's meetings and discussion sessions with various CBSL departments and divisions.

## EXECUTIVE SUMMARY

**The CBSL has been working on improving its risk management function since 2015.** The central bank has a detailed risk governance framework in place, including a high-level Risk Management Policy Statement (RMPS), and is working towards implementing an Enterprise Risk Management framework.

**The creation of the BROC<sup>2</sup> and Non-Financial Risk Management Committee (NFRMC) is a key step in promoting risk discussions at the appropriate level.** As these are recently established Committees, there is some room for improvement in their current functioning, as detailed further in this report.

**The CBSL has established various foundational aspects for proper risk management.** The mission's recommendations are aimed at further embedding the risk management function within the CBSL, to extend its efforts, and to improve the CBSL's risk culture.

**The Bank should strengthen the “tone at the top.”** The planned adoption of a (top-down) risk appetite statement (RAS) will improve risk ownership at all levels of the organization. The CBSL should also ensure specific training (including at the top management level) and effective communication/awareness actions.

**Empowerment of the risk management function should similarly continue to be supported.** This should include more active participation by the risk management function in monitoring progress of the strategic plan, supporting strategic risk assessments (SRA) (top down), and participating in key CBSL meetings and projects.

**Additionally, the CBSL should pursue proper implementation of the 3 Lines Model.** This includes providing further clarification of the roles and responsibilities of business units (first line), risk management (second line), and internal audit (IA) (third line).

**The CBSL should similarly define the appropriate risk tolerance levels.** This would need to be done through a proper definition of Key Risk Indicators (KRIs), and can accelerate the path towards a more mature risk management function.

**Overall, a more strategic approach to risk management is needed.** Progressing towards a stronger risk management culture is a long term objective. It requires clear ownership by the Governing Board (GB), allowing alignment between the CBSL's strategy and objectives and the risk management function. Ultimately, this will lead to a better-informed, more efficient and effective CBSL decision-making process, in line with the CBSL's legal mandate.

---

<sup>2</sup> The BROC was created by the CBSL's Monetary Board. If, down the line, changes to the CBSL Act are considered, the authorities could consider including an explicit reference to the BROC in the Act.

**Table 1. Key Recommendations**

Recommendations		Priorities	Timeframe	Lead Actors
<i>A. Risk Management Governance</i>				
1	CRO formally reports to BROC, through NFRMC and has administrative only reporting to AG. <b>CRO should report to a DG (or to the Governor) and/or interact more directly with the NFRMC Chair.</b> This should be formalized, together with (eventually) tailored reporting and frequent one-on-one meetings. (Paragraph 12)	High	Immediate <3 months	GB
2	SRA is a direct responsibility of the Monetary Policy Board (MPB) and the GB. <b>The RMD should be more involved in this process and in the strategic planning.</b> MPB and the GB should manage this type of risk in a structured manner, including through identifying key risks regarding strategic planning, with support of the RMD. SRA should follow international best practices, being a top/down exercise, with ownership by GB/BROC. (Paragraph 13)	High	Short term <12 months	GB
3	The CBSL should continue to <b>explore an enhanced Human Resources (HR) strategy</b> to attract, reward, and retain staff in all critical areas (e.g., risk and cybersecurity). (Paragraph 14)	High	Short term <12 months	GB
4	The RMD has limited participation in pre-decision stages of the decision-making process:  (i) <b>The RMD should have mandatory participation in all relevant Committees</b> (such Information Technology (IT) Oversight Committee, MP Committee and BCP Committee).  (ii) <b>The GB should promote further alignment and involvement of RMD in Business Continuity Planning (BCP).</b> (Paragraph 15)	Medium	Immediate <3 months  Short-term <12 months	GB  GB, RMD, BCP Committee
5	<i>(Follow-up of Safeguards Assessment)</i> <b>The CBSL cybersecurity function needs to be advanced with dedicated and specialized resources.</b> The cybersecurity framework should also be strengthened, including through proper information-sharing with the RMD. (Paragraph 16)	High	Immediate <3 months	GB, IT Department
6	<b>Organize a 1.5-day IMF Governing Board Workshop for executive and nonexecutive members of the GB.</b> This would allow detailed interaction with Board members on key aspects of central bank governance, legal framework, risk management & cybersecurity, audit committee (AC), operational efficiency, and transparency—with a focus on their respective roles and responsibilities. (Paragraph 17)	Medium	Medium term 12-24 months	GB
<i>B. Risk Management Framework and Appetite</i>				
7	<b>Continue developing the RM Framework</b> , covering all CBSL risks, including through a RAS (top down). (Paragraphs 27, 28)	High	Short term <12 months	GB, RMD
8	<b>Optimize BROC time, focusing on implications and mitigation of risks. Frequency of meetings should adhere to the formally defined: quarterly.</b> Particular attention should be given to top/strategic risks and/or significant	High	Short term <12 months	BROC, NFRMC, RMD

	escalations from NFRMC. Both committees need more pre-engagements with the first line (business departments). (Paragraph 30)			
9	<b>Continue to develop the KRI process</b> , starting by clearly defining its objectives and positioning and a more objective framework. Support the first line in the definition of KRIs (significant, clear, and objective) aligned with RAS and in a reduced/controlled number. (Paragraph 29)	High	Short term <12 months	All business units, RMD
10	<b>Implement Risk Management integrated Reports</b> , with sharp (i.e., focus on weaknesses), concise, updated, and timely information, reconsidering Risk and Control Self-Assessment (RCSA) frequency scoring/levels. An effective communication strategy should help to prioritize and better visualize risks and support risk management decisions. (Paragraph 31)	Medium	Ongoing	BROC, NFRMC, RMD
11	<b>Expedite the procurement process of the Risk Management System</b> for improvement of efficiency of the risk management process and risk reporting. (Paragraph 32)	Medium	Short term <12 months	Procurement Committee, Relevant Business Units
<i>C. Strengthen the Three Lines Model</i>				
12	<b>Clearly define information-sharing between second and third lines</b> , specifying the type and frequency of the information to be exchanged between the lines. (Paragraph 41)	Medium	Immediate <3 months	RMD, IAD
13	<b>Business units should have greater awareness of their role as first line and their contribution to the RMD.</b> Risk Coordinating Officers (RCOs) should have specific RM training and bank-wide meetings organized by RMD, to share best practices/lessons learned from risk events and/or with external speakers. (Paragraphs 42, 43, 44)	Medium	Short term <12 months	All business units, RMD
14	<b>Promote a closer relationship with the International Operational Risk Working Group (IORWG), Central Bank Risk Managers (CBRM) and enhance bilateral cooperation</b> with other central banks and International Financial Institutions (IFIs) to guarantee permanent alignment with international best practices. (Paragraph 45)	Medium	Immediate <3 months	RMD



## I. INTRODUCTION

- 1. The CBSL’s Risk Management Department (RMD) was created in 2015.** After two years, in 2017, the scope of the RMD was extended, and operational risk management was incorporated into the RMD in line with the Three Lines Model. In 2023, the RMD completed the facilitation for development of risk registers of all 29 business units of the CBSL.
- 2. In 2022, an IMF Safeguards Assessment<sup>3</sup> flagged the need for further improvement of the CBSL’s risk management function.** This resulted in a request for TA from the CBSL to MCM.
- 3. The MCM TA mission received a significant amount of information.** The mission’s engagement spanned two months, and included six days of onsite meetings and presentation sessions with various staff members of the CBSL. This greatly facilitated the team’s assessment of identifying main areas for improvement. The next sections will outline the mission’s findings and recommendations in more detail.

## II. RISK MANAGEMENT GOVERNANCE

### A. Current Situation

- 4. The key policies and governance of the risk management function are consistent and robust.** The mission analyzed, I.A, the RMPS, Risk Management Framework, Operational Risk Management Guideline (ORMG), samples of the agenda and minutes of the BROCC and NFRMC, IA recommendations, and Risk Registers—see Appendix I for a complete overview of documents shared with the mission. In general, the relevant risk management documents and information produced are consistent and robust, and a risk governance structure is present.
- 5. However, implementation of the risk management framework and appetite is not fully completed.** Relevant documents and policies are quite recent and lack a certain amount of maturity. Understandably, establishing a proper risk culture throughout the central bank takes time. RCOs, who serve as risk liaisons between the first line (business departments) and the second line (RMD) are critical. However, their role, profile, and training needs are not sufficiently outlined in risk management documentation and CBSL policies.
- 6. The risk management function is governed by an approved RMPS.** A revised RMPS was approved by the Monetary Board (MB) in January 2023. The RMD is responsible for financial and operational risks. The RMD currently comprises nine staff members directly involved with risk management-related activities, as well as three management level staff, and three existing vacancies. With regard to operational risk, the RMD reports to the GB through the

---

<sup>3</sup> Central Bank of Sri Lanka – 2022 – IMF Safeguards Assessment Report, February 27, 2023.

(NFRMC) and the BROCC; for financial risk, the RMD reports to the GB through the BROCC<sup>4</sup> (Figure 1). The BROCC meets quarterly. However, over the last two years, due to a lack of quorum, the BROCC was not able to meet as frequently. Accordingly, the RMD reported to the NFRMC (operational risks). The current RMD reporting line does not facilitate regular access by the CRO to top management, which limits the opportunities to discuss strategic issues and/or to get specific feedback on risk management reporting.

**7. Several elements of the risk management process have been implemented.** This includes incident management—facilitated by an online incident reporting system accessible to all staff, and risk mapping for the whole bank. On the other hand, key elements such as developing a risk appetite framework (RAF) have not been fully addressed, though they have been identified as a priority with a defined development plan, including the approval of a RAS at the GB and the definition of KRIs for all risk categories (this is currently in development).

**8. The strategic planning process is well-established.** This process is coordinated by the Policy Review and Monitoring Department on an annual basis, with the involvement of senior management and GB. The process has evolved over recent years and is quite extensive. Nonetheless, the RMD has not been fully involved with the preparation of the CBSL’s Strategic plan (which runs till 2026), through the SRA of objectives. Furthermore, conversations with the RMD revealed limited participation of risk management in pre-decision stages of the CBSL decision-making process, which is critical for determining whether to proceed with various initiatives.

**9. Staffing is currently a top risk for the CBSL.** The number of resignations has grown from 5 people in 2020, 14 in 2021, 51 in 2022, to approximately 40 (year-to-date) in 2023. This is likely a more generic problem at the country-level, but it also impacts the ability of the CBSL in particular to deliver on its goals. Critical CBSL positions are unfilled (for instance, one DG, and various AGs). This significantly impacts the CBSL’s activity in a negative manner. The CBSL has hired an external consultant to develop specific mitigation plans, which are expected to be rolled out over the next two years. Control functions such as risk management, compliance, and cybersecurity are significantly and negatively impacted by these current HR constraints. The team was also informed of additional impacts of this risk in the staffing of core critical functions, as a consequence of recent amendments to Banking Act.

**10. Cyber risk management has room for improvement.** Though awareness and training has evolved in this field, CBSL cyber risk management still has significant room for further improvement. There is no Chief Information Security Officer (CISO), even though the recruitment process is in place, and a proper and dedicated monitoring structure has not yet been

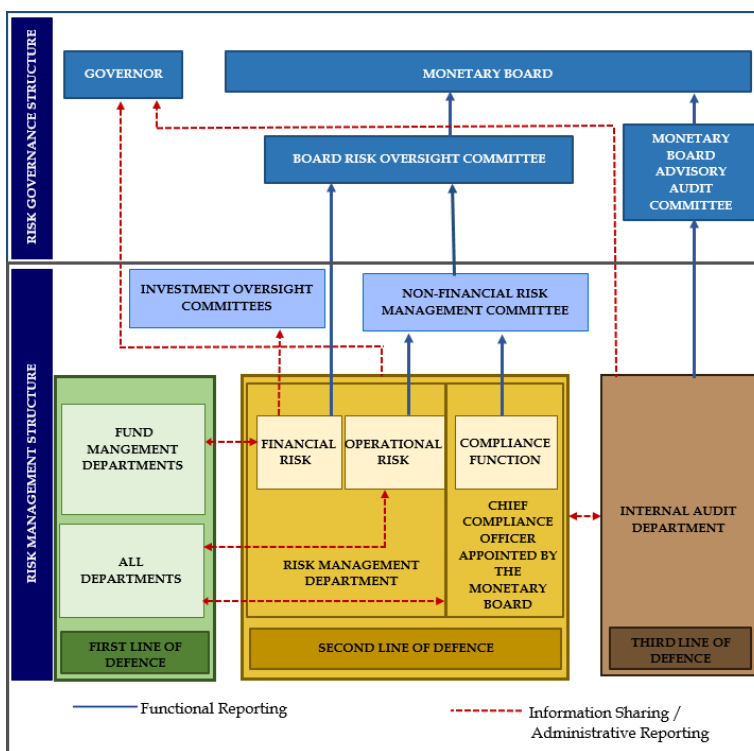
---

<sup>4</sup> The BROCC is chaired by an independent Board member, nominated by the Board, and also comprises two independent external experts, as well as several observers (a SDG/DGs, CCO, Chief Internal Auditor, CRO and Director and Chairman of the Committee for Disaster Recovery).

implemented—there is a plan to implement a Security Operations Center and KRIs will be defined as part of the RAS plan, but this needs to be operationalized further

**11. Certain second line functions are a cause for concern.** The process to monitor and report conduct risks is currently ad-hoc and not formalized/well-defined. Additionally, the Compliance Function does not have sufficient resources (the Chief Compliance Officer (CCO), is only employed part-time and has a shared full time employee (50 percent) with the CBSL’s Legal Department), nor is the function sufficiently independent.

**Figure 1. Risk Management and Governance Structure of the CBSL**



Source: Central Bank of Sri Lanka.

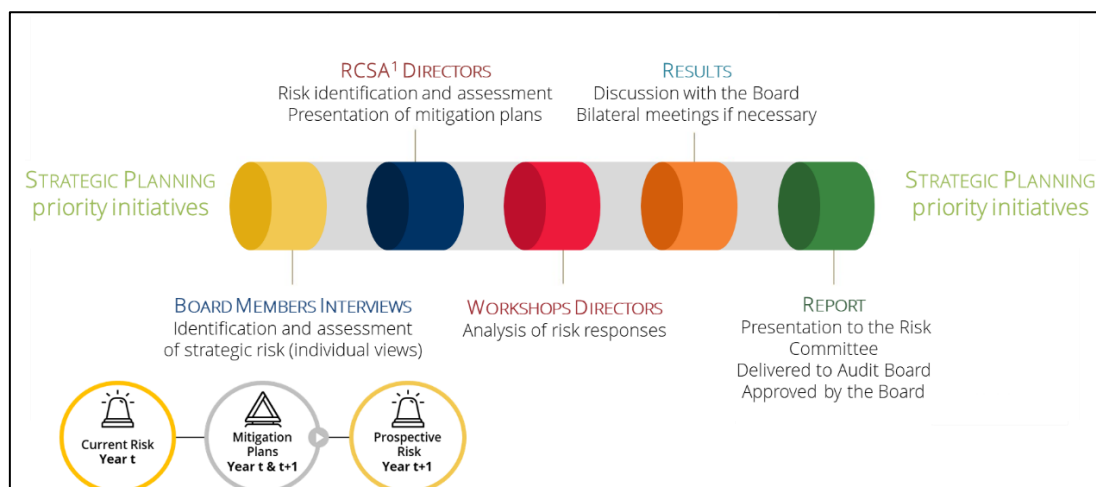
## B. Recommendations

**12. The CRO should report to a DG (or to the Governor) and/or to interact more directly with the Chair of the NFRMC.** This process should be properly formalized, together with (eventually) tailored reporting and frequent one-on-one meetings. This clarification can help to improve top management ownership of risk management, and will also speed up consistent and frequent feedback on the RMD’s activities and plans.

**13. SRA is a direct responsibility of the MPB and the GB.** The RMD should be more involved with assessing strategic risks, and, accordingly with the overall strategic planning process. The MPB and GB should improve management of strategic risk, by including identification of top/ key risks in relation with strategic planning, with the support of the RMD.

A reflection on emerging risks should also be a part of the BROCC agenda. An SRA should be set up in line with international best practices (see Figure 2 for a structured example), being a top/down exercise, with ownership by GB/BROCC. BROCC discussions should focus on strategy-related issues, instead of purely tactical ones.

**Figure 2. Strategic Risk Management**



Source: Banco de Portugal.

**14. The CBSL should continue to explore an enhanced HR strategy to attract, reward, and retain staff in all critical areas (e.g., risk and cybersecurity).** The current HR plan should be delivered as soon as possible, and should include mitigating actions to retain staff and draft proper succession plans for all critical CBSL functions. Staffing of internal control functions, such as cybersecurity, risk management, compliance, and business continuity, is critical and should be prioritized in the HR strategy.

**15. RMD participation in pre-decision stages of the decision-making process should be increased.** The RMD should have mandatory participation in all relevant committees (such as the IT Oversight Committee, Monetary Policy Committee, and BCP Committee). The GB should promote further alignment and involvement of the RMD in BCP (in line with international best practices). RMD early involvement will allow for proper management of risks of critical CBSL processes/projects.

**16. CBSL's cybersecurity function needs to be advanced with dedicated and specialized resources.** The cybersecurity framework should also be strengthened, including through information-sharing with the RMD. The CBSL should complete the recruitment of the CISO and have separate resources dedicated to handling cybersecurity. The mission feels that additional IMF support could help to speed up the process, as well as allow the CBSL to benefit from international standards and best practices.

**17. The CBSL should organize a 1.5-day IMF Board Workshop for executive and nonexecutive members of the GB.** Such a workshop would allow detailed interaction with

executive and nonexecutive Board members on key aspects of central bank governance, legal framework, risk management & cybersecurity, AC, operational efficiency, and transparency—with a focus on their respective roles and responsibilities. Participation of AGs could also be considered, to improve knowledge of key concepts and ensure alignment with management throughout the CBSL.

### III. RISK MANAGEMENT FRAMEWORK AND APPETITE

#### A. Current Situation

**18. The CBSL has been on a multi-year journey of building out its risk management function.** The CBSL created the RMD in 2015, with a focus on financial risk only. The Bank gradually expanded its risk management scope, and in 2017 an operational risk function was added along the lines of the Three Lines of Defense Model.<sup>5</sup> The RMD is the central point of the risk management function at the Bank, and is managed by the head, two deputies and nine staff members.

**19. The CBSL has developed a comprehensive RMPS which was approved by the MB.** The document is reviewed biannually and may be changed based on the RMD's proposal, and/or NFRMC/BROC recommendations to the GB. The RMPS describes the risk taxonomy (Figure 3), the risk management process (based on ISO 31000-2018), responsibilities and reporting lines of all three lines, roles of CRO, CCO, Departmental Risk Officers (DROs), RCOs, and other stakeholders, composition of the committees (including BROC and NFRMC), and so on. The scope of the RMPS covers financial, operational, strategic, and compliance risks. In practice, the CBSL has not yet developed a strategic risk framework, and a compliance risk function is still at the early stages of development.

**20. Risk registers for all business units are completed and approved by the MB.** The RMD has created a risk register template in line with the methodology described in the ORMG approved by the Board. Risk assessment is done using a qualitative method based on the methodology and expert judgements of the first and second lines. The process of filling out risk registers for individual business units started in 2019, and as a result of RMD's partnership with all 29 business units, the risk registers for all business units of the bank was completed in Q1 of 2023. A consolidated operational risk profile was submitted to the GB and approved in Q3 of 2023. The methodology chosen by the CBSL and described in the ORMG meets international best practices and is coherent with the majority of other central banks.

**21. Risk registers are updated quarterly, but no concise and formalized RCSA process is exercised.** The ORMG clarifies the frequency of risk register updates. Each business unit should review the risks, risk ratings, controls and treatments quarterly and should submit non-

---

<sup>5</sup> <https://www.theiia.org/globalassets/documents/resources/the-iiias-three-lines-model-an-update-of-the-three-lines-of-defense-july-2020/three-lines-model-updated-english.pdf>

financial risk events (internal and external), emerging risks, significant operational risks and status of action plans to the RMD on a quarterly basis through the departmental risk register. The limited resources of the RMD (two persons in charge of operational risk) and the collection of risk registers for 29 business units on a quarterly basis may turn this practice into a mechanical and routine process, with lacking in-depth analysis and interactions between the first and second lines as a consequence.

**22. The CBSL does not use a proper system for its operational risk management process.** Based on the operational risk assessment methodology chosen by the CBSL, the RMD created a risk register template in a standardized format in Microsoft Excel. The creation, update, and consolidation of risk registers is done in spreadsheets. However, this method can lead to human errors and the risk of losing data, which may complicate the preparation of relevant risks registers and reports in an accurate and timely manner. Further automation of these processes seems to be something the CBSL intends to develop. The Bank decided on procuring a Governance, Risk and Compliance system, but at the time of the mission this process was still pending.

**23. All staff members of the CBSL have a duty to report incidents, including near misses.** An online Incident Reporting System has been established, accessible to staff at all levels, where the identity of the person reporting an incident is completely protected (unless the submitting staff member indicates differently). The RMD has developed training material for incident reporting, which consists of a comprehensive and clear step-by-step guide for usage of the incident system. The training material (Incident Reporting System User Guideline) outlines clear and correct messages along the lines of the “intention of the incident reporting is NOT to blame or shame individuals or departments, but to strengthen the control environment and ensure that incidents are informed on time, enabling appropriate responses to minimize negative impacts and future occurrences ...” and it is “purely an improvement endeavor which will NOT be used for any disciplinary actions against persons reporting incidents (originators).” However, there is no formal document outlining the goal, importance, and principles of incident reporting. In practice, this leads to reporting of ‘incidents’ that would ideally not be classified as operational risk incidents.

**24. The RMD, together with the business units, has started developing KRIs.** At the time of the mission, the RMD had developed KRIs for three sub-categories of operational risk categories: (i) cyber security risk; (ii) human resources risk; and (iii) system and technology risk. However, for these KRIs the threshold values (acceptable ranges) still need to be defined. According to the ORMG, business units should submit actual values for each KRI identified to the RMD on a quarterly basis, prior to the NFRMC meeting. The mission notes that this process is still in the early stages within the CBSL, could be strengthened further, including through more detailed guidelines and principles. During the mission, and at the request of the RMD, the mission had detailed discussions with the team on the process of developing KRIs, defining relevant risk limits/thresholds for KRIs, monitoring performance against risk limits, the link

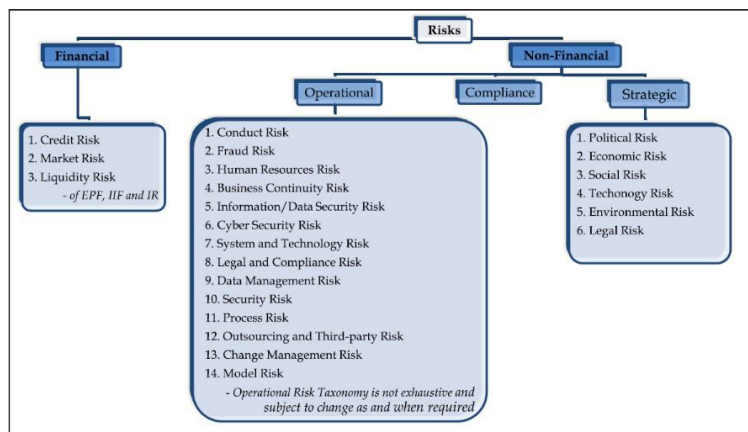


between KRIs and RAS, review and update of KRIs, a detailed RAS and its frequency, and so on.

**25. The Bank has approved a Concept Paper on “Developing a Risk Appetite Framework for the Central Bank of Sri Lanka.”** The document describes the vision for the development and implementation of a RAS, as well as the roles and responsibilities of the stakeholders in this process. Consistent with best practices, this statement will be approved by the GB of the CBSL. Based on the roadmap for RAS implementation, the timeline for submitting the RAS, recommended by the BROCC, for the approval of the GB is the 4<sup>th</sup> quarter of 2024. The RMD has done comprehensive work and conducted a detailed study of other countries’ central banks’ RAS and submitted a report to the NFRMC and BROCC on the proposed RAF for CBSL. During the onsite mission, the mission team shared the experience of their central banks’ RAS (i.e., Portugal and Georgia) with the RMD team, as well as the study “Risk Appetite Statement and Tolerance Repository” developed by the IORWG in 2022.

**26. The RMD formally reports its activities to the NFRMC and the BROCC on a quarterly basis.** Based on the data submitted by the business units, the RMD prepares the aggregate dashboard and reports for the quarter for discussion at the NFRMC and BROCC. The aggregate report includes: top operational risks; key highlights, messages and actions for the quarter; and other operational risk categories. Additionally, the RMD submits quarterly reports with details of the incidents and near-misses to the NFRMC and BROCC. Regarding information on critical incidents reported by the business units, the RMD should immediately notify it to the Chairman of the NFRMC. NFRMC and BROCC meetings last for two to five hours, and there are cases when the meeting is adjourned for another day. Each meeting is documented in very detailed committee minutes. The mission noted that there is a need for further alignment before committee discussions take place, to facilitate discussions and enhance efficiency. There is also a need among internal stakeholders for more engagement by some Directors of Departments. Other stakeholders note that a simpler/high-level risk dashboard would be beneficial.

**Figure 3. Risk Taxonomy of the CBSL**



Source: Central Bank of Sri Lanka.

## B. Recommendations

**27. The support of the risk function currently provided by CBSL senior management should be formalized through the adoption of a RAS (top down).** The statement would re-affirm that the CBSL is willing to operate within a “low risk range,” while it is at the same time willing to accept some risks, to the extent that it advances its mandate of achieving price and financial stability.

**28. Development of the Risk Management Framework should continue, covering all risks managed at the CBSL, including a RAS.** The RAS should be approved by the GB and/or MPB of the CBSL, as appropriately and be revisited and reinforced periodically. The risk appetite can be formalized through a set of qualitative or quantitative parameters and statements. The RAS supports transparency among stakeholders (internal and external) as to how the Bank manages certain risks. The risk appetite levels will guide senior management in decision-making and will form the basis for a well-defined risk profile.

**29. The KRI process should be developed further, starting by clearly defining its objectives, positioning, and a more objective framework in general.** With RMD leadership and guidance, support should be given to the first line in the definition of KRIs (significant, clear, and objective). The mission recommends establishing KRIs aligned with the RAS in a reduced/controlled number. The threshold values (acceptable ranges) for KRIs should be carefully developed based on expert judgement, taking into consideration past experience and current and future trends. In the process of implementing KRIs, it should be ensured that they are clearly understood by all three lines and senior management, and supported with reliable data sources from appropriate information systems.

**Figure 4. Key Risk Indicators**



Source: Banco de Portugal.



**30. BROC time should be optimized, focusing on the implications and mitigation of risks.** Frequency of meetings should always be quarterly, as formally defined. BROC members' time should be utilized effectively—in the meetings, particular attention should be given to top operational, financial and compliance strategic risks, critical incidents, and/or significant escalations from the NFRMC. The effective work of both committees (BROC and NFRMC) depends significantly on the quality of risk management reporting. To achieve this, it is important that the RMD is supported by timely and accurate data. Further pre-engagements with the risk owners (first line) are critical.

**31. Risk Management integrated reports should be implemented with sharp (i.e., focus on weaknesses), concise, updated, and timely information.** The frequency of RCSAs should be reconsidered taking into account scoring/levels. Consideration should be given to further development of a more standardized RCSA with a multi-year plan to cover the whole Bank, in close interaction between the first and second lines. Finding the optimal frequency for updating risk registers will support the RMD in saving use of their resources for further development of risk management communication. An effective communication strategy should help to prioritize and better visualize risks and support risk management decisions. The manual work involved with the CBSL's risk assessment process could hamper further improvement. The planned automation could help to improve the entire risk management process as well as risk reporting, allowing for more unified and tailored risk reporting.

**32. The procurement process of the Risk Management System for the improvement of the efficiency of the risk management process and risk reporting needs to be expedited.** The Bank's risk management function will have reached a sufficient level of maturity when it has moved from Microsoft Excel spreadsheets to a proper risk management system. Establishing a holistic approach to risk management can be supported through an integrated system (which would include risk management, incidents, action tracking, KRIs, controls assessment, etc.). In the process of development (or selection) of the system, it will be important for the CBSL to find synergies (and an improved cost-benefit analysis) with other functions, such as IA, business continuity management, and compliance management.

#### **IV. STRENGTHENING THE THREE LINES MODEL**

##### **A. Current Situation**

**33. The CBSL is using a Three Lines Model approach to risk management.** The RMPS defines the application of this model, where the roles and responsibilities are distributed among business units (first line), RMD (second line), and the Internal Audit Department (IAD) (third line). The CBSL has been on a journey to improve its risk management practices, which is reflected in a growing risk awareness and culture. As part of this progress, the Three Lines Model's implementation is, however, still not fully embedded.

**34. There is no clear definition of the type and frequency of information-sharing between the second and the third lines.** Information-sharing between lines is not formalized

and is mainly done through the representation of heads of departments in the various committees. The Chief Internal Auditor is an observer on the BROCC and NFRMC; the CRO is an observer on the AC. In practice, the RMD shares risk registers with the IAD upon their request. The IAD should share information about audit findings with the RMD. This may require formalization from the GB, as CBSL Act notes that IA reports of the Bank shall not be shared with anyone other than the person authorized by the GB.<sup>6</sup>

**35. The IAD is accountable to the AC of the CBSL.** The IA function should provide independent assurance to the GB/MPB and support it. CBSL senior management should promote an effective risk management process. At the time of the mission, with the AC in wait of a new chairperson, the team did not have the opportunity to interview AC members, making it difficult to determine the AC level of oversight over the IA and risk management functions.

**36. Interaction between the RMD and the first line has improved over the last few years, but there is still room for improvement.** The mission notes that cooperation and alignment could be intensified. As the first line, business units should be aware that they are the risk owners and have a key role in managing their own risks, and realize the added value the second line has for their current risk management practices. Discussions with departments suggest that the degree of ownership of this aspect of the function is uneven. There is a notion that risk awareness and knowledge, at the first line level, could be improved and standardized. This includes further engagement from Directors of Departments and AGs.

**37. For each business unit, a person (RCO) is designated to support risk related responsibilities of the DRO, who is the focal point to conduct risk management activities.** The RCOs assist the business units to manage their risks and closely coordinate with RMD to carry out the risk management process effectively. Business units, supported by the RCOs should submit non-financial risk events (internal and external), emerging risks, significant operational risks and status of action plans to RMD every quarter through the Departmental Risk Register.

**38. The RCOs' potential role is not fully explored.** The RCOs exist but lack visibility and consistency in relation with the RMD. The profile of RCOs is not consistent in all CBSL business units. Additionally, there is no detailed and updated job description for this critical risk management role. Though the roles and responsibilities are defined by the relevant document, the RCOs are not actively and fully used by the RMD in practice. RCOs can add value to the improvement of the risk management process and, accordingly, the RMD should provide them with training/sharing of best practices or lessons learned and facilitate continuous improvement of their risk management skills.

**39. The CBSL actively cooperates with other central banks on risk management.** The RMD has established bilateral cooperation with the Bank Al Maghrib, the South African Reserve Bank, and - recently – the Bank of Portugal. The CBSL is a member of the IORWG, however, in

---

<sup>6</sup> Central Bank of Sri Lanka Act, Article 103, Paragraph 7.

recent years, they have been less involved in the IORWG’s activities and have not participated in the annual conferences. This could be improved, as the IORWG is the most appropriate platform for central banks’ operational risk management knowledge-sharing, self-development, and benchmarking.

## **B. Recommendations**

**40. The Three Lines Model should be further enhanced and formalized at all possible levels.** Overall, staff should be aware of their detailed individual roles and responsibilities regarding the internal control environment. “The Three Lines Model” helps organizations identify structures and processes that best assist the achievement of objectives and facilitate strong governance and risk management.”<sup>7</sup>

**41. There should be a clear definition of information-sharing between the second and the third lines.** The type and the frequency of the information to be exchanged between the lines should be specified and formalized. Information-sharing between the second (i.e., RMD, Compliance and Information Security) and the third line (i.e., IAD) should be promoted to strengthen the consistency and efficiency of the internal control environment. As an example, risk assessments should tie into the IA plan, as well as RCSAs should take IA recommendations into account. Also, IAD information on effectiveness of controls in place could be very helpful for RMD, especially when there are gaps in the respective design.

**42. Business units should have a greater awareness of their role as the first line and contribution of the RMD.** The first line is the first responsible party for managing risks, using the available resources and following any guidance from the second and third lines. The CBSL needs to foster this awareness by facilitating adequate and sufficient resources, particularly at the business level. Cooperation on risk management between the business units, their DRO/RCO (as the first line) and the RMD (as the second line) allows a two-way conversation as to how risks are being seen, managed and where necessary mitigated. A quick and transparent escalation process is needed, as well as the increased importance of the current DROs/RCOs in each business unit in assessing controls, anticipating vulnerabilities and helping with mitigation strategies. This will allow more uniform/less distinct views on risk management issues and will contribute to a more efficient use of resources.

**43. DROs and RCOs should have specific RM training and bank-wide meetings organized by RMD, to share best practices/lessons learned from risk events and/or with external speakers.** The RMD should organize and sponsor specific and regular risk management sessions and meetings for RCOs to discuss methodology, report templates, case studies and lessons learned. A strong interaction between the RMD and the RCOs will increase the awareness of the business units, enhance buy-in for risk management, and consequently,

---

<sup>7</sup> <https://www.theiia.org/globalassets/documents/resources/the-iias-three-lines-model-an-update-of-the-three-lines-of-defense-july-2020/three-lines-model-updated-english.pdf>

strengthen the overall risk culture of all the staff in the CBSL. RCOs should be engaged in a consistent and more intense manner, to improve the risk management process. The risk management framework should also emphasize the particular role of RCOs, who should act as an extension of the RMD within their respective business units.

**44. The role of RCO needs to be formalized.** Formalization of the RCOs could be done via clear job descriptions, including a list of tasks that the RCOs need to undertake. Ideally, this would form the basis for the annual performance review input of the RCO. The respective manager of the RCO would also seek review input from the RMD.

**45. The CBSL should promote closer relationships with the IORWG, CBRM Group, and bilateral cooperation with other central banks and IFIs.** This will support additional research and benchmarking in risk management with other central banks. The active participation in working groups and conferences will provide the CBSL with additional and updated information to guarantee alignment with international best practices. Proper attention should also continue to be dedicated to the development of the RMD team as this is a function that requires recurrent and updated knowledge in several areas, from technical to soft skills (communication, negotiation, etc.).

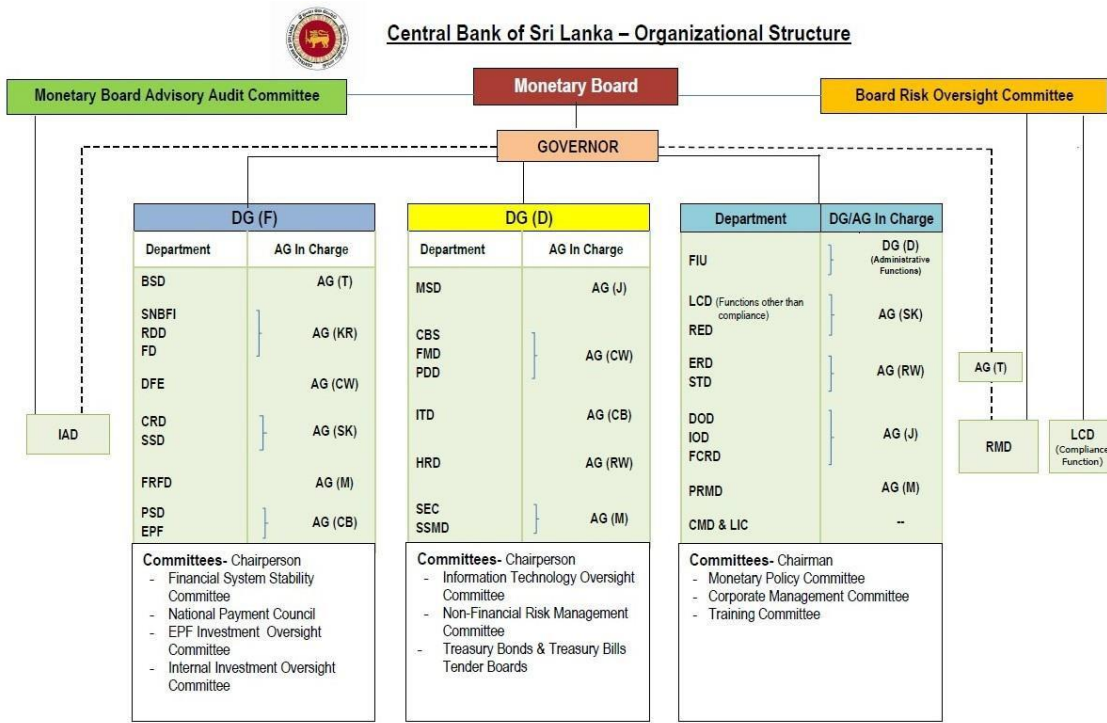
## APPENDIX I. LIST OF THE DOCUMENTS SHARED WITH THE MISSION

1. Central Bank of Sri Lanka Act No. 16 of 2023.
2. Concept Paper – Developing a Risk Appetite Framework for the Central Bank of Sri Lanka, Annex 1.
3. Central Bank of Sri Lanka – Organizational Structure.
4. Risk Management and Governance Structure.
5. Description of the functions of the departments of CBSL.
6. CBSL Operational Risk Profile.
7. CBSL Strategic and Action Plan – 2023.
8. Draft Key Risk Indicators (KRIs) for Cyber Security Risk.
9. Draft Key Risk Indicators (KRIs) for System and Technology Risk.
10. Draft Key Risk Indicators (KRIs) for Human Resources Risk.
11. Risk Register Template.
12. CBSL Risk Management Policy Statement, Third revision approved by the MB.
13. Agenda of the NFRMC #21, June 21, 2023.
14. Minutes of the NFRMC #21, June 21, 2023.
15. Presentation for NFRMC meeting – Update on ORM, March 16, 2023.
16. Agenda of the BROCC #17, May 12, 2023.
17. Minutes of the BROCC #17, May 12, 2023.
18. Presentation for BROCC meeting – Update on ORM, October 5, 2023.
19. Incident Reporting System – User Guideline.
20. Operational Risk Management Guideline.
21. The Monetary Board Minute Paper on ORM function progress.
22. Meeting Agenda of the Committee for Contingency Events and Disaster Recovery for LankaSettle October 2, 2023.
23. Minutes of the Meeting of the Committee for Contingency Events and Disaster Recovery for LankaSettle System, October 2, 2023.
24. Business Continuity Plan (Payment and Settlement Department)
25. Draft Internal Audit Report, November 10, 2023.
26. Awareness Presentation to DROs and RCOs – “Implementing a Risk Appetite Framework for CBSL.”
27. Presentation – “The BCP process for the LankaSettle system and related critical systems.”

## APPENDIX II. LIST OF PEOPLE MET

1. Dr. P. Nandalal Weerasinghe – Governor.
2. Mrs. T. M. J. Y. P. Fernando – Senior Deputy Governor.
3. Mrs. K. M. A. N. Daulagala – Deputy Governor.
4. Mr. Trevine Jayasekara – BROC Independent External Member.
5. Mr. H A Karunaratne – BROC Independent External Member.
6. Mr. A. A. M. Thassim - Assistant Governor.
7. Mr. C. P. S. Bandara – Assistant Governor, Chairman of BCP Committee.
8. Mr. K. G. P. Sirikumara – Assistant Governor, Chief Compliance Officer.
9. Mr. W R M K Fernando – Head of Risk Management Department.
10. Mrs. R D T Gunasekara – Head of Policy Review and Monitoring Department.
11. Mrs. D. K. Mayadunna – Head of Internal Audit Department.
12. Mr. H. M. P. B. Herath – Head of Information Technology Department.
13. Officers of Risk Management Department.
14. Departmental Risk Officers (Heads of Department).
15. Risk Coordinating Officers.

### APPENDIX III. ORGANIZATIONAL CHART OF THE CBSL



Functional Reporting ————— Administrative Reporting - - - - -

19.10.2022

## APPENDIX IV. BOARDS OF THE CBSL

### Governing Board

1	Governor, Chairperson	Dr. P. Nandalal Weerasinghe
2	Appointed Member	Mr. Vish Govindasamy
3	Appointed Member	Mr. Nihal Fonseka
4	Appointed Member	Dr. Ravi Rathnayake
5	Appointed Member	Mr. Anushka Wijesinha
6	Vacant	
7	Vacant	

Source: Central Bank of Sri Lanka official website, January 2024

### Monetary Policy Board

1	Governor, Chairperson	Dr. P. Nandalal Weerasinghe
2	Appointed Member	Mr. Vish Govindasamy
3	Appointed Member	Mr. Nihal Fonseka
4	Appointed Member	Dr. Ravi Rathnayake
5	Appointed Member	Mr. Anushka Wijesinha
6	Vacant	
7	Vacant	
9	Appointed Member	Dr. Dushni Weerakoon
10	Appointed Member	Prof. Priyanga Dunusinghe
11	Sr. Deputy Governor	Mrs. T. M. J. Y. P. Fernando
12	Deputy Governor	Mrs. K. M. A. N. Daulagala

Source: Central Bank of Sri Lanka official website, January 2024



**APPENDIX V. RISK COMMITTEES OF THE NBSL**

**Board Risk Oversight Committee (BROC)**

1	Chairperson, Appointed Member	Mr.Nihal Fonseka
2	Independent External Member	Mr. H. A. Karunaratne
3	Independent External Member	Mr. Trevine Jayasekara
4	Observer, Senior Deputy Governor	Ms. T. M. J. Y. P. Fernando
5	Observer, Deputy Governor	Mrs. K. M. A. N. Daulagala
6	Observer, Assent Governor, Chief Compliance Officer	Mr. K. G. P. Sirikumara
7	Observer, Assent Governor, Chairman of BCP Committee	Mr. C. P. S. Bandara
8	Secretary, Assistant Governor	Mr. A. A. M. Thassim
9	Assistant Secretary, Observer, Convener, Director of Risk Management Department	Mr. W. R. M. K. Fernando
10	Observer, Chief Internal Auditor	Mrs. D. K. Mayadunna


Source: Central Bank of Sri Lanka.

**Non-Financial Risk Management Committee (NFRMC)**

1	Chairperson, Deputy Governor	Mrs. K. M. A. N. Daulagala
2	Member, Senior Deputy Governor	Ms. T. M. J. Y. P. Fernando
3	Member, Assistant Governor	Mr. J. P. R. Karunaratne
4	Member, Assistant Governor	Mr. A. A. M. Thassim
5	Member, Assistant Governor	Mr. A. R. K. Wijesekara
6	Member, Assistant Governor, Chief Compliance Officer	Mr. K. G. P. Sirikumara
7	Member, Assistant Governor, Chairman of BCP Committee	Mr. C. P. S. Bandara
8	Secretary, Director of Risk Management Department	Mr. W. R. M. K. Fernando
9	Observer, Chief Internal Auditor	Mrs. D. K. Mayadunna,

Source: Central Bank of Sri Lanka.

## APPENDIX VI. PRESENTATION FROM THE MISSION



**IMF TA Mission to the Central Bank of Sri Lanka**

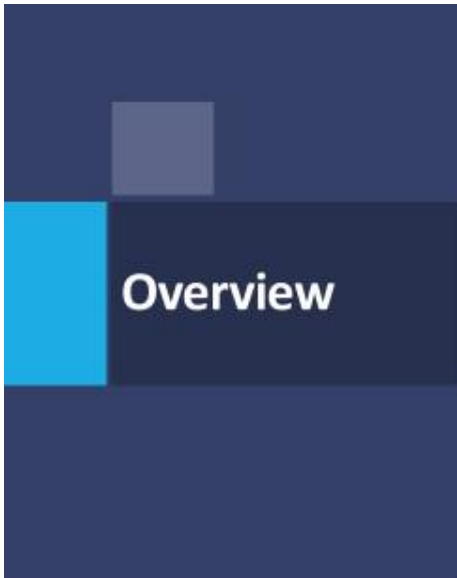
**PRESENTATION TO THE CBSL ON DRAFT RECOMMENDATIONS**

December 4, 2023

Gabriel Andrade and Mariam Manjgaladze

Monetary and Capital Markets Department (MCM)

1



**Overview**

- 
1. Introduction
  2. Mission team and objectives
  3. Recommendations A: Risk Management Governance
  4. Recommendations B: Risk Management Framework and Appetite
  5. Recommendations C: Strengthen the Three Lines Model
  6. Next steps
  7. Q&A

**DISCLAIMER**  
The views expressed here are those of the IMF's staff, and not necessarily those of the IMF's management or Executive Board.

**COPYRIGHT**  
This material is the property of the IMF and is intended for use only by IMF staff.

2

# Introduction

Today's presentation

## Presentation today

- Overview of draft recommendations based on
- (i) Desk review of risk management documents (October - November 2023);
- (ii) Meetings with CBSL staff members (November 27 – December 1, 2023)

## Would not have been possible without:

- RMD team: Mahinda, Thilini, Gayal, Arunie, Nishantha, Nimna and all others
- Monetary Policy Board members, BROCC independent external members, Assistance Governors, Directors and other staff members that generously freed up time!

3

# Mission Team and Objectives

## Mission Team:

**Ashraf Khan** (Activity Lead, IMF Monetary and Capital Markets Department)

**Gabriel Andrade** (IMF Short-Term Expert, Bank of Portugal)

**Mariam Manjgaladze** (IMF Short-Term Expert, National Bank of Georgia)

## Mission Objectives:

- To provide technical support and guidance to the Central Bank of Sri Lanka to further improve its own risk management.

4

## Recommendations

Recommendations		Priorities
<b>A. Risk Management Governance</b>		
	CRO formally reports to BROCC, through NFRMC and has administrative only reporting to AG.	
1	CRO should report to a Executive Monetary Policy Board Member and/or to interact more directly with the Chair of the NFRMC. This should then be correctly formalized, together with (eventually) tailored reporting and frequent one-to-one meetings.	High
	Strategic Risk Management (SRA) is a direct responsibility of the MB. RMD is not involved in this process nor in strategic planning.	
2	MB should manage this type of risk in a structured way, including identifying key risks in relation with strategic planning, with the support of RMD. SRA should follow international best practices, being a top/down exercise, with ownership by MB/BROCC.	High
3	CBSL should continue to explore an enhanced HR strategy to attract, reward, and retain staff in all critical areas (e.g. risk and cybersecurity).	High

5

## Recommendations

Recommendations		Priorities
<b>A. Risk Management Governance</b>		
	RMD has limited participation in pre-decision stages of the decision-making process:	
4	(i) RMD should have mandatory participation in all relevant Committees (such IT Oversight Committee, MP Committee and BCP Committee).  (ii) MB should promote further alignment and involvement of RMD in the Business Continuity Planning (international best practice)	Medium
5	(Follow-up of Safeguards Assessment) CBSL's cybersecurity function needs to be advanced with dedicated and specialized resources. The cybersecurity framework should also be strengthened, including information sharing with RMD.	High
6	Organize a 1.5-day IMF Governing Board Workshop for executive and nonexecutive members of the Governing Board. This would allow detailed interaction with Board members on key aspects of central bank governance, legal framework, risk management & cybersecurity, audit committee, operational efficiency, and transparency – with a focus on their respective roles and responsibilities in these areas.	Medium

6

## Recommendations

Recommendations		Priorities
<i>B. Risk Management Framework and Appetite</i>		
7	Continue developing the RM Framework that should cover all risks managed at CBSL, including Risk Appetite Statement (top down).	High
8	Optimize BROC time, focusing on implications and mitigation of risks. Particular attention should be given to top/strategic risks and/or significant escalations from NFRMC. On both Committees, further pre-engagements with 1 <sup>st</sup> lines.	High
9	Continue to further develop KRI process, starting by clearly defining its objectives and positioning and a more objective framework. Support the 1 <sup>st</sup> line in the definition of KRIs (significant, clear, objective) aligned with RAS and in a reduced/controlled number.	High
10	Implementing Risk Management integrated Reports, with sharp (i.e. focus on weaknesses), concise, updated and timely information, reconsidering RCSA frequency scoring/levels. An effective communication strategy should help to prioritize and better visualize risks and support risk management decisions.	Medium
11	Consider the implementation of a Risk Management System for improvement of efficiency of the risk management process and risk reporting.	Medium

7

## Recommendations

Recommendations		Priorities
<i>C. Strengthen the Three Lines Model</i>		
12	Clearly define information sharing between 2nd and 3rd lines, specifying the type and frequency of the information to be exchanged between the lines.	Medium
13	Business units should have greater awareness of their role as 1st line and contribution of RMD. Risk Coordinating Officers should have specific RM training and bank-wide meetings organized by RMD, to share best practices / lessons learned from risk events and/or with external speakers.	Medium
14	Promote closer relationship with IORWG and bilateral cooperation with other central banks and IFIs to guarantee permanent alignment with international best practices.	Medium

8

## Next Steps

1. Discussion / feedback today
2. Fine tune recommendations on owners and planned dates with RMD
3. Draft TA report (December-January)
4. Internal IMF review
5. Finalized TA report
6. Follow-up with IMF further works (to be determined)

9

## Q & A

10