WP/19/303

IMF Working Paper

Risk Management Maturity Assessment at Central Banks

by Elie Chamoun, Nicolas Denewet, Antonio Manzanera
and Sanjeev Matai

INTERNATIONAL MONETARY FUND

 WP/19/303

IMF Working Paper

Finance Department

Risk Management Maturity Assessment of Central Banks

Prepared by Elie Chamoun, Nicolas Denewet, Antonio Manzanera and Sanjeev Matai[1]

Authorized for distribution by Simon Bradbury

December 2019

Abstract

Effective risk management at central banks is best enabled by a sound framework embedded throughout the organization that supports the design and execution of risk management activities. To evaluate the risk management practices at a central bank, the Safeguards Assessments Division of the IMF's Finance Department developed a tool that facilitates stocktaking of elements that are present and categorizes the function based on its maturity. Tailored recommendations are then provided to the central bank which provide a roadmap to advance the risk management function.

Keywords: central banks, risk management, maturity assessments

Author's E-Mail Address: EChamoun@imf.org, NDenewet@imf.org, AManzanera@imf.org and SMatai@imf.org

[1] We would like to thank Simon Bradbury and George Kabwe for their review and insightful comments. The authors are also grateful to staff in the IMF Monetary and Capital Markets Department (MCM), Office of Internal Audit (OIA) and Office of Risk Management (ORM) for their review and valuable comments. The views expressed in this paper are solely those of the authors, and do not purport to represent those of the IMF, its Executive Board, or IMF management. All errors and omissions are our own.

Table of Contents

I. INTRODUCTION

When the IMF provides financing to a member country, a safeguards assessment is carried out to obtain reasonable assurance that the country's central bank is able to manage the Fund's resources and provide reliable monetary data on the IMF-supported program. Safeguards assessments are diagnostic reviews of central banks' governance and control frameworks, and involve an evaluation of central bank operations in five areas: the **E**xternal audit mechanism, the **L**egal structure and autonomy, the financial **R**eporting framework, the **I**nternal audit mechanism, and the system of internal **C**ontrols, denoted by the acronym ELRIC.[2]

The safeguards assessment framework was adapted in 2010 to include a review of the risk management practices as an integral part of the system of internal controls. Initially, this was limited to reviewing and stocktaking the existence and attributes of basic risk management structures, and in 2015 the approach was intensified to include a deeper evaluation of risk management functions and their effectiveness.[3]

Considering risk management does not have universal international standards, a phased approach was adopted to implement this new requirement. A benchmarking review of widely used risk management frameworks was conducted to distill the core elements of a fully-fledged risk management framework. A second phase then took into consideration the different levels of implementation of central bank risk management functions to develop a maturity spectrum. The two phases culminated in the development of the maturity assessment toolkit.

The assessment toolkit was developed to guide the evaluation of risk management practices at central banks in a structured and comprehensive manner, and to facilitate consistent and tailored recommendations for a modular progression in maturity. As such, it combines a periodic checkpoint and a path forward to continue developing the risk management practices.

The paper is structured as follows. Section II provides an overview of the multi-stage methodological approach that culminated in the creation of the tool. Section III describes the common elements of a strong risk management framework. Section IV introduces the maturity level concept to guide the assessment of risk management practices. Finally, Section V provides a description and illustrative examples of the tool to evaluate the maturity of risk management practices in a central bank.

---

[2] The safeguards policy is an integral part of the IMF's risk management framework for its lending activities, with 311 assessments covering 97 central banks completed as of April 2019. More information on the IMF safeguards policy is available at: *Safeguards Factsheet*

[3] In its 2015 review of the safeguards policy, the Executive Board of the IMF recognized, inter alia, the importance of integrated risk management frameworks in strengthening institutions, and called for a broader coverage in this area, tailored to each central bank's capacity.

II. METHODOLOGICAL APPROACH

During the 2015 review of the safeguards policy, the IMF Executive Board endorsed an external review panel's recommendation to sharpen the focus of safeguards assessments on risk management at central banks.[4] This represented a new policy requirement and entailed a shift from the previous approach adopted in 2010 towards the assessment of risk management functions at central banks. Initially, such assessment was limited to that of conducting a stocktake of the extent to which a central bank had developed an integrated risk management function. As risk management is demanding from a conceptual and technical perspective, the breadth and maturity of risk management functions depend largely on the central bank's capacity. Central banks are at different stages of maturity in adopting enterprise-wide risk management operations.[5] Experience under the safeguards policy indicates that few central banks have a full-fledged risk management framework. Further, given that there is no "one size fits all", challenges in deciding on an appropriate framework for implementation are widespread.

In order to implement this new policy requirement, a phased approach to assessing risk management frameworks at central banks was adopted. As risk management is a relatively new or evolving function at many central banks, we have found that frameworks differ across central banks and regions. As a result, the first step was to establish common elements of a risk management framework to serve as a benchmark for evaluating risk management practices in safeguards assessments. The next step was to introduce a maturity model approach, providing high-level guidance on determining the maturity level of these practices. The last step was the development of a tool to assess risk management practices in order to make tailored safeguards recommendations. The tool is a matrix combining both the elements of the risk management framework and the attributes for each maturity level of each of the elements (see Annex I for a detailed description of the tool).

While the accounting and audit industries are guided by international standards, risk management does not have a single universal standard that is widely applied.[6] Central banks with advanced risk management functions acknowledge that the choice of components in implementing a framework is driven by the unique circumstances and environment in which the bank operates. The current available risk management guidelines include: (i) *ISO 31000:2018, Risk management – Guidelines* (provides principles, framework and a process

---

[4] *Safeguards Assessments - Review of Experience* and *Safeguards Assessments Policy - External Expert Panel's Advisory Report*

[5] Per *COSO Enterprise Risk Management – Integrated Framework (2004)*, "Enterprise risk management is a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives."

[6] Certain guidelines and principles for specific central banking functions exist such as the *IMF Guidelines for Foreign Exchange Reserve Management* and the *BIS Principles for Financial Market Infrastructures*.

for managing risk and can be used by any organization regardless of its size, activity or sector); and (ii) *COSO Enterprise Risk Management—Integrating with Strategy and Performance* (highlights the importance of considering risk in both the strategy-setting process and in driving performance). Our stocktaking of central banks since 2010 found that these were the most widely used (see Annex II for a detailed description of both guidelines).[7]

The benchmarking risk management framework was then defined based on the ISO and COSO guidelines. It includes the broad concepts and common elements that are expected to be found in a strong risk management framework (see below).

III. RISK MANAGEMENT FRAMEWORK[8]

The following section provides a description of the benchmarking framework as the foundation for risk management.[9] It outlines the common elements of an enterprise-wide approach to identifying, measuring, monitoring, and managing risk across the central bank. Broadly defined, this framework is also the most effective way to delineate the principles and cultural aspects that should govern the coordinated practices for risk management.

A. High-Level Principles

Effective risk management practices are guided by the following high-level principles:

- **Accountability**: Risk management is facilitated through a clear mandate and a comprehensive approach as an integral part of all activities.
- **Robust governance**: Risk management roles and responsibilities are well defined with clear reporting lines, providing for independence from operations and adequate "checks and balances" at all levels, including Board oversight.
- **Proportionality:** Risk management is enabled by a dedicated structure (framework and processes) that is tailored to a central bank's risk profile and operational environment, and maturing along with other organizational processes.
- **Adequate resources:** The risk management function should have appropriate capabilities to fulfill its mandate, including the right mix of skills, competencies, tools and systems.
- **Transparency and effective communication:** Risk management maintains a systematic and timely monitoring and reporting on risk exposures and action plans at all levels.
- **Assurance and continuous improvement**: Risk management is dynamic and continually improved with experience and periodic reviews (e.g., audits and external assessments).

---

[7] In addition, the International Operational Risk Working Group (IORWG), a global forum dedicated to advancing the management of operational risk in the central banking industry, produces guidelines of topical interest for its members.

[8] This section draws extensively on common leading practices in risk management, in particular (i) *ISO 31000:2018, Risk Management-Guidelines*, and (ii) COSO Enterprise Risk Management- Integrating with Strategy and Performance as the main sources of the benchmarking exercise.

[9] As defined in *ISO 31000:2018*, risk management is the "coordinated activities to direct and control an organization with regard to risk (the effect of uncertainty of outcomes)".

B. Risk Culture

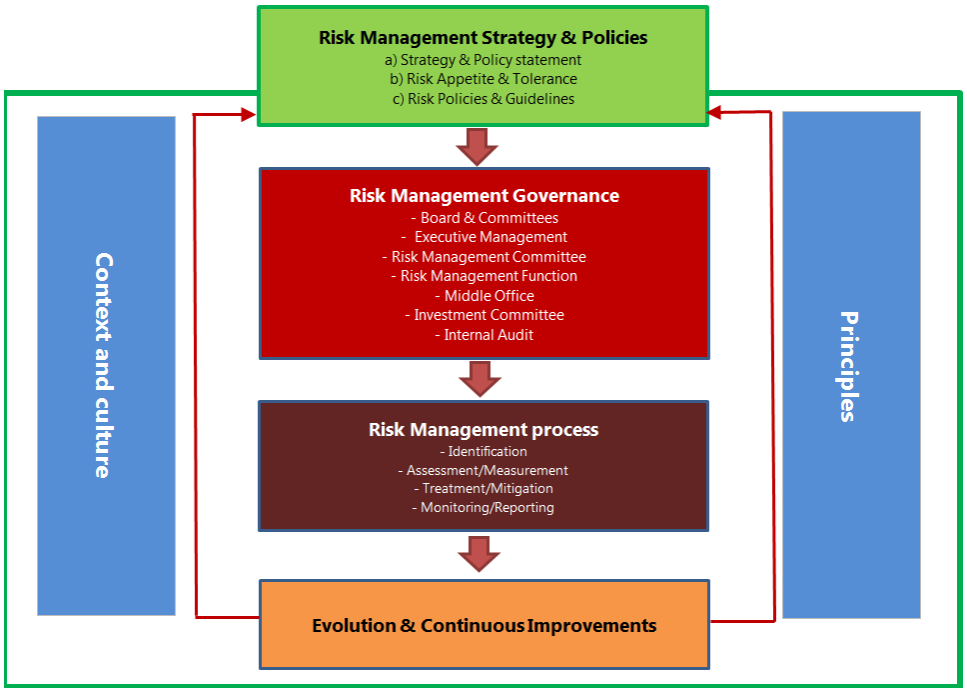
Complementing the high-level principles is the risk culture advocating for the right tone at the top and promoting risk awareness as a foundation for sound risk management. For example, the right risk culture bolsters effective risk management; promotes sound risk-taking; and ensures that emerging risks and excessive risk-taking activities are assessed, escalated and addressed in a timely manner.[10] This places risk culture at the intersection of behavior and risk management. Despite the recent focus on risk culture, it remains at initial stages of development and substantial work is yet to be done in this area.[11]

C. Risk Management Framework – Common Elements

The initial step in evaluating the risk management practices in the context of a safeguards assessment at a central bank is a benchmarking exercise to determine whether (i) a systematic approach to risk management has been adopted, and (ii) it is facilitated by a strong risk management framework incorporating the key elements expected to be found in leading practices (shown in Figure 1).

Figure 1. Risk Management Framework – Key Elements

Effective risk management is best enabled by a sound framework embedded throughout the central bank that supports the design and execution of risk management activities.



Source: IMF Staff - *"Integrated Risk Management-Common Elements"* - adapted

[10] Illustrative objectives extracted from the "Guidance on Supervisory Interaction with Financial Institutions on Risk Culture - A framework for assessing risk culture": Financial Stability Board, April 2014.

[11] This observation draws on safeguards experience at central banks assessed under the IMF safeguards policy and the review of risk management related literature, including on risk culture.

Risk management strategy, policies and guidelines

The risk management strategy, usually approved and adopted by the highest governing body such as the Board of the central bank, describes the high-level objectives and scope of risk management. It also serves to define the risk culture of the institution and is communicated through a formal and concise umbrella document.

Risk appetite and tolerance levels are also determined at this level, i.e., approved by the Board, and are expressed through qualitative statements and quantitative indicators, and then communicated down to the operational levels.[12, 13]

The risk management strategy is further delineated in a set of specific policies and guidelines detailing the approach to the management of each type of risk. It also documents the roles and responsibilities of the stakeholders involved in the management of risks, and outlines key aspects of the risk management processes, tools and methodologies, including reporting lines and requirements.

Risk management governance

A governance structure for the management of risks should strike a balance between the ultimate responsibility and oversight at Board level, and risk ownership for the day-to-day activities at operational level. It would typically include the following stakeholders: (i) the Board, responsible for defining the overall risk strategy and exercising oversight of risk management (sometimes via a dedicated Board Risk Committee or the Audit Committee);[14] (ii) Executive Management, assuming the overall responsibility for the management of risks;[15] (iii) the risk management function, an independent department in charge of facilitating the process of identification, assessment, monitoring and reporting of risks;[16] and (iv) the internal audit function, providing independent and objective assurance on the effectiveness of risk management.[17]

---

[12] Risk appetite: the broad level and type of risk a financial institution is willing to take in pursuit of its strategy and objectives. In theory, this represents the extent of risk that the financial institution would be able to assume and safely manage over an extended time horizon, which in turn is reflected in its policies, processes and procedures around key functions/activities.

[13] Risk tolerance: the acceptable levels of deviation from the Board-approved risk appetite. These levels are difficult to determine and need to be specific for each function of the bank.

[14] While governance arrangements differ amongst central banks, reference to "Board" in this paper relates to the highest governing (oversight) body of the central bank.

[15] Executive Management sometimes delegates some responsibilities to a dedicated committee, such as an Investment Committee or a Risk Management Committee.

[16] Separation between financial and non-financial risk management is common, with in some cases the Middle Office taking responsibility for the management of financial risks.

[17] This broad structure mirrors the three lines of defense model, in which the business areas perform the first control activities embedded in the operations, the risk management is responsible for the second layer of controls and compliance, and the internal audit provides an independent assurance on the adequacy of the control systems.

Risk management process

This is a set of coordinated activities that cycles continuously through the process of: (i) risk identification – the inventory and classification of all risks the central bank is exposed to; (ii) risk assessment – the analysis and measurement of the identified risks; (iii) risk treatment – the selection and implementation of a risk mitigation strategy; and (iv) risk monitoring and reporting – the mechanisms to continuously monitor and report risk exposures and risk events to the relevant stakeholders. The risk management process should be rigorously documented and periodically evaluated.

Evolution and continuous improvements

The independent assessment of the risk management framework plays a crucial role in its continuous evolution and improvement, and helps ensure that it remains adequate and effective over time. This can be achieved through independent periodic reviews performed by internal (e.g., internal audit) or external parties (e.g., consultants or peer central banks).

IV. Maturity Spectrum

A. Maturity Stages of Risk Management Practices

Adopting a framework is the first step in establishing a risk management practice. However, the nature of implementation varies across central banks. The maturity model approach to assessing risk management practices assumes that the quality and depth of these practices should evolve and improve with time, following a pathway of development stages. This is indeed what has been observed in practice where such frameworks grow organically over a period of time. Table 1 provides a broad classification of the four maturity levels used to determine the adequacy and effectiveness of risk management practices for safeguards assessment purposes:

Table 1. Risk Management Framework Maturity Levels

Maturity Level	Description
Informal and unstructured	Nonexistent or very weak function with no structured approach for risk management practices. Risk management may be at an initial stage (conceptual) and mostly not supported by a formal framework or dedicated resources.
Developing	Initiated but function not fully developed. The elements of risk management are defined (in form) but not yet implemented through a formal established process and structure.
Implementing	Present but still fragmented. A risk management approach is implemented and most tools and techniques are effectively functional; additional work is required to ensure overall integration of risk management practices within the activities of the central bank.
Optimized	Risk management is mature and has been embedded in the operations of the central bank. All elements of the framework are consistently applied and continuously evolving with the profile of the central bank.

Source: IMF Staff - *"Maturity Progression of Risk Management Practices at a Central Bank – Assessment Guidance"*.

A key feature of this maturity assessment is that the various stages occur in sequence and that the central bank has the ability to progress from one level to the next. However, it should be noted that: (a) certain components may evolve more quickly than others; (b) a desired level of maturity is a function of the central bank's risk profile, culture, domestic environment, investments needed to move to higher levels of maturity, and potential benefits; and (c) it is not necessary, and may not even be possible, to achieve the highest level of maturity for all components. In addition to the cost/benefit considerations, the evolution along the maturity continuum is a journey influenced by capacity considerations and the availability of adequate resources.

B. Considerations for Maturity Progression of Risk Management

The working assumption of this paper is that a maturity level can be determined based on assertions of completeness, adequacy, and consistency in application of the key components laid-out in Section III. As such, the recommendations on how central banks can strengthen risk management practices and facilitate a gradual evolution from one level to another on the maturity scale should be guided by the following considerations:

- **Desired state of maturity**. This is typically the extension of central banks' commitment to risk management, which is influenced by their risk appetite and tolerance levels.
- **Closing gaps**. The focus should be on actions that will achieve the greatest impact in terms of progression. However, in deciding on the pace of the evolution, the central bank should always take into consideration capacity constraints.
- **Integration**. Embedding risk management processes across the central bank should be a continuous process rather than a one-off annual exercise. Ultimately, risk assessment and management would become a routine element of policy design and implementation.

V. MATURITY ASSESSMENT TOOL

The Maturity Assessment Tool (MAT) is a combination of the benchmarking framework and the maturity model approach (see Annex I).

A. Definitions, Objectives and Design of the Maturity Assessment Tool

The MAT is a tool designed internally by the Safeguards Assessments Division of the IMF's Finance Department to be used in the context of safeguards evaluations. Its objective, as described above, is twofold: (i) evaluate the development status of the risk management function relative to all the elements of a risk management framework, and (ii) provide a basis for the identification of development needs and recommendations.

It is important to distinguish the purpose of the creation of the MAT from other objectives. In particular, while the MAT is not necessarily intended to be a self-evaluation tool, central banks may use it to guide the implementation of their risk management frameworks or

identify improvement needs to align the quality of their existing risk management functions with leading practices.

The MAT is a matrix: (i) the **rows** contain the elements of the risk management framework described in Section III, and (ii) the **columns** list the maturity levels introduced in Section IV. Within the matrix, each cell provides a high-level description of the status of an element of the risk management framework, for a given maturity stage. In other words, the MAT describes the **attributes** that each element of the framework should display so that it can be determined as adequate for that level of maturity (see Annex I for illustration).

As an example, with respect to governance and an instance where a Risk Management Committee is not established, the MAT indicates that for the level of maturity of a central bank to be considered at least "developing", “oversight of risk management activities is ensured through other governance arrangements (e.g., Audit Committee) on ad-hoc basis.”

B. Use of the Maturity Assessment Tool

The MAT is used as a guide during safeguards assessments to facilitate a comprehensive coverage of all the elements of the risk management framework.

For each element of a central bank risk management framework, the activities are mapped to the descriptions that the MAT provides for each level of maturity. This mapping allows the determination of the level of maturity of that specific element. Once the level of maturity has been identified, recommendations to progress to the next level are derived from the description offered by the MAT for that element.

The overall maturity level of a central bank’s risk management practices will be determined according to the preponderance of attributes under each level and will require a non-mechanistic judgement that takes into consideration all relevant attributes observed in the central bank.

C. Illustrative Examples

This section provides illustrative examples on the use of the MAT, each described in a table with three columns:

- The first column contains a **hypothetical response** obtained from the central bank;
- The second column presents the **description** offered by the MAT that best matches that response; and
- The third column offers a **possible recommendation** to facilitate a modular transition to the next maturity level.

Example 1: Risk Appetite

The risk appetite is a key element in risk management because it identifies the risks that will be tolerated ex ante (i.e., will not require specific treatment, such as mitigation plans).

Description obtained from the central bank	Best fit relative to expected attribute in the MAT	Possible recommendation to the central bank
"The central bank has a definition of risk appetite that we use inside our department. This is enough because we are the experts…"	"Risk appetite is not articulated in a formal statement" ("developing")	The central bank should define and approve a risk appetite statement to be approved by the Board and communicated down to the operational levels (*see description in "implementing" stage*).

Example 2: Risk Management Committee (RMC)

The RMC is a governance body comprising senior executives whose responsibilities include, inter alia, monitoring of risks, oversight of risk exposures and advising the Board on risk management issues.

Description obtained from the central bank	Best fit relative to expected attribute in the MAT	Possible recommendation to the central bank
"Even if our RMC lacks a charter, it is composed of all Heads of Department and meets once a year. During the last meeting, important issues relating to the physical security of our main building were discussed…"	"The RMC exits but its operations are not optimal: For example, (i) its members lack requisite skills, (ii) absence of clear mandate, (iii) low frequency of meetings or random agendas" ("implementing")	The central bank should enhance its RMC by appointing senior executives with relevant expertise and approving a charter containing its mandate and responsibilities (*see description in "optimal" stage*).

Example 3: Risk Treatment / Action Plans

Risks that are outside of the risk appetite and tolerance levels will require a treatment. In some instances, a mitigation plan will be required, according to the risk tolerance.

Description obtained from the central bank	Best fit relative to expected attribute in the MAT	Possible recommendation to the central bank
"We identify new controls to mitigate major risks. The Head of the Department is in charge of their implementation. This responsibility falls within his purview, and he may decide to develop an action plan…"	"Risk treatment / mitigation measures have been identified for some risks, but not converted into formal action plans and no mechanism to ensure their implementation and for assessing their effectiveness" ("developing")	The central bank should develop and record action plans to implement mitigation measures, and establish a process to monitor their implementation (*see description in "implementing" stage*).

Example 4: Risk Management Annual Report

Annual risk reports are usually prepared for the oversight body. The report highlights all relevant developments in the function and contains a detailed description of the evolution of the central bank's risk profile.

Description obtained from the central bank	Best fit relative to expected attribute in the MAT	Possible recommendation to the central bank
"Our Board is informed immediately on all important issues relating to risk management, such as major incidents. In these instances, the risk management department elaborates a detailed report containing all relevant information…"	"The oversight body is informed on *ad-hoc* basis" ("developing")	The risk management department should provide a summary of the department's activities in an annual report and present it to the oversight body. The report should include the risk management strategy and the description of the risk profile of the central bank (*see description in "implementing" stage*).

Example 5: Risk quantification

Central banks should quantify risks to better assess their financial impacts and provide for adequate buffers. In this example, the central bank is in the informal stage and we present two possible recommendations: move towards the developing stage, or progress by two levels to the implementing stage.

Description obtained from the central bank	Best fit relative to expected attribute in the MAT	Possible recommendation to the central bank
"We do not quantify risks, neither financial risks, nor operational risks…"	"No quantification" ("informal")	1. The central bank should quantify financial risks as a first step (*see description in "developing" stage*). 2. The central bank should acquire the skills and tools to quantify both financial and operational risks (*see description in "implementing" stage*).[18,19]

[18] Operational risk is defined in the *2005 Revised Basel II Framework* as "The risk of loss resulting from inadequate or failed internal processes, people, and systems or from external events."

[19] While not widely applied among central banks, the quantification of operational risks is an indicator of an advanced level of maturity, as it requires a certain level of sophistication in terms of skills and tools.

VI. CONCLUSION

Risk management continues to evolve as an important function in strengthening the system of internal controls of central banks. Safeguards experience indicates that central banks have begun with implementation of such functions, but the differences observed in their level of maturity are widespread. The Maturity Assessment Tool which the Safeguards Assessments Division of the IMF's Finance Department has developed should assist in moving central banks' risk management functions forward through an evaluation of the progress made in operationalizing key concepts and facilitating gradual improvement.

ANNEX I: RISK MANAGEMENT MATURITY ASSESSMENT TOOL **Maturity Stages**				
	Informal	**Developing**	**Implementing**	**Optimized**
Risk Management Strategy and Policies				
Strategy & Policy				
Senior management's (Board and executive management) commitment and approach to risk management	The Central Bank has no formal risk management strategy, no policy and no integration with other processes. No dedicated resources committed to risk management.	Senior management commits some resources to risk management. Senior management provides input into the approach to risk management and reviews the risk management framework on an ad-hoc basis. Risk management activities are aimed at risk avoidance.	Senior management promotes the risk management framework across the central bank (e.g., annual reports). It makes explicit its risk appetite and tolerance to risk. Ownership of risk management is vested in a senior executive and is appropriately resourced. There is some evidence of risk management being factored into senior management's decision-making processes. Risk analysis performed in big projects / initiatives.	Senior management demonstrates ongoing commitment to risk management (developments, adequate resources, attending conferences) and its continual improvement with new tools, software, training, etc. Dedicated section on risk management in the strategy planning process. Senior management drives the integration of risk management at both strategic and operational levels (e.g., strategic planning and decision-making processes) through an organic, systematic approach.
Risk Management Strategy and Policy	No formal risk management strategy is in place. The central bank has no risk management policy.	The risk management strategy is limited to broad guidance on basic matters such as risk identification (and register) and reporting arrangements. The approach to risk management is embedded in other established policies for departmental business activities. Risk Management policy is high level.	There is a risk management strategy providing specific guidance on the scope and governance of risk management, including risk identification and prioritization, risk appetite and risk mitigation and reporting. The central bank has a formal policy that defines the scope of, and delineates the responsibilities for, risk management across the central bank. The policy is endorsed by the Board and executed by a dedicated risk management function. Some elements of the framework are stated in the policy, but they are not fully implemented.	The risk management strategy outlines the central bank's approach to risk management and defines its risk appetite. It also includes the roles and responsibilities for risk management, outlines the risk management process, and defines how risks will be evaluated and the process for monitoring and reviewing risk management periodically. The risk management strategy is publicized throughout the central bank and made available to all staff. This involves sending updates and holding awareness and training sessions frequently. The risk management strategy is reviewed annually. The central bank has a formal policy based on international standards and kept up to date. In addition to the scope of risk management and related responsibilities, the policy

ANNEX I: RISK MANAGEMENT MATURITY ASSESSMENT TOOL **Maturity Stages**				
	Informal	**Developing**	**Implementing**	**Optimized**
				makes reference to the risk appetite statements and relevant risk tolerance levels, and outlines the way risk management performance (KRIs) will be measured and reported. The risk management policy provides clearly for how risk management decisions will be made and communicated. All elements of the framework are described in the policy in a clear and comprehensive manner.
Risk taxonomies	No taxonomies.	Some definitions informally taken as taxonomies. They are informally understood and used.	Defined taxonomies incorporated in formal guidelines.	Taxonomies are clearly identified and incorporated in risk management guidelines. The Bank classifies different sorts of risks and manages them in an integrated/standardized manner. Besides cultural concepts, the organization has a common glossary of terms and definitions so that everyone has the same understanding of risk language.
Risk Appetite				
Risk Appetite Statement(s) and Tolerance Levels	No risk appetite defined.	Risk appetite is not articulated in a formal statement.	Risk appetite is defined and approved as a formal statement and communicated through the Board.	The risk appetite statements provide clarity around how the central bank will take on or avoid certain risks or outcomes in pursuit of its business. The risk appetite is also formalized through a set of quantitative metrics and qualitative statements. The risk appetite and related tolerance levels are considered by senior management in decision-making. The risk appetite and tolerances are revisited and reinforced periodically as part of the periodic review of the risk profile of the central bank.

Maturity Stages				
	Informal	**Developing**	**Implementing**	**Optimized**
Risk integration	RM is not integrated with any other process.	Risk management is not integrated, but plans are under way to integrate with other areas / processes. Risk management is informed about business continuity work and vice versa, but there is little coordination between both. IT risks are identified and assessed as other common risks using the same methodology.	Risk management is integrated, at least with IT, audit plans, training planning, budget planning, etc. There is some coordination, for example BCM uses risk management information to schedule its work and risk management monitors risks related to critical processes. Risk management outcomes normally taken into consideration for some topics (e.g. inputs in the strategic process) and/or operational and tactical decisions in the strategy planning process. There is a separate methodology to identify and assess IT risks, conducted by specialized IT staff.	Risk management is embedded in all core processes of the central bank. In particular, it is an integral part of the strategic planning and decision making process. Risk management is not simply considered as an operational issue, but is also taken into account when developing policies and broad strategies. Besides integration with operational and tactical plans, it is also used to establish accountability and integrated within strategic planning (if in place) and top management decision-making. It is a continuous activity and viewed as a key element of good governance. Risk management is an integral part of project and program planning. Risk management and BCM are fully integrated. They share tools and participate in each other planning by providing inputs and suggestions. Teams meet regularly and risk management participates on BCM drills. A risk management analysis is conducted for all IT projects / applications using a separate methodology to identify and assess all risks (those stemming from projects and those pertaining to applications). Risk management is a core part of the IT function, and there are specialized IT staff taking care of IT risk management.

Maturity Stages				
	Informal	**Developing**	**Implementing**	**Optimized**
Risk Governance and Accountability				
Risk Management Structure				
Board	There is no dedicated risk governance structure in place. The Board's responsibility for risk oversight is not defined.	There is a risk governance structure, but risk reporting lines and accountabilities are not established directly to the Board. The Board receives key information regarding risk management issues on an ad-hoc basis.	The Board 1) periodically receives risk management reports, and 2) is aware of major risk management issues. The Board 1) approves the risk policy and risk appetite statements, and 2) oversees implementation of the risk management framework.	The Board's responsibility related to risk management is clearly articulated in its charter or its By-laws. The Board 1) approves the risk policy and risk appetite statements, 2) oversees implementation of risk management framework at all levels of the central bank, and 3) evaluates and reviews the policy in light of results achieved. Risk management reports are received periodically by the Board and risk management issues are a permanent item on the agenda of Board meetings.
Executive (senior) Management	Executive management responsibilities for risk management are not formally defined or articulated.	The Risk Management Function is embedded in another function and led by the executive in charge of that other organizational unit (e.g. Internal Audit, General Control, Operations, Compliance, etc.). Moreover it lacks exposure to senior management.	The risk management function is led by a senior staff who is not a member of the Executive Management team and does not have previous risk management experience.	The head of risk management is a member of the Executive Management team of the central bank (equivalent of a Chief Risk Officer function). The Executive in charge has extensive experience in risk management. There is a designated risk management body responsible for an independent governance structure with direct reporting lines and accountabilities to the Board/Committee/Executive Management.
Risk Management Committees	There is no dedicated committee for risk management.	There is no risk management committee, but oversight of risk management activities is ensured through other governance arrangements (e.g. Audit Committee) on an ad-hoc basis.	There is a risk management committee, but its operations are not optimal: for example (i) its members lack requisite skills, (ii) absence of clear mandate, (iii) low frequency of meetings or random agendas.	There is a fully operational Executive Risk Management Committee with a clear mandate and well-defined overall responsibilities. The committee is composed of senior executives (including a Deputy Governor) with relevant expertise that also contributes to the improvement of the risk management function and advises the Board in discharging its

Maturity Stages				
	Informal	**Developing**	**Implementing**	**Optimized**
				oversight of risk management issues.
Risk Management Function				
Risk Management Function (Unit/Department)	The central bank does not have a central risk management team or dedicated risk management unit. The three lines of defense model is not implemented.	There is a risk management team, but its objectives, scope and responsibilities are not specified. The boundaries between the three lines are not clearly defined. There is duplicative and inefficient work. The risk management unit is not organizationally independent (e.g. part of the Control Department, or the Finance Department).	There is a central risk management unit with formal responsibilities, and clear objectives, scope and reporting lines. However, staff's skills can be improved. While the boundaries between the second and third lines of defense are clearly defined, there is little or no cooperation between on risk issues (for example between internal audit and risk management).	The dedicated risk management unit (division/department) is administratively and functionally independent with direct line to senior management (Board and executive management). The boundaries are defined, and roles and responsibilities are well understood. There is regular communication between the three lines of defense. An effective accountability mechanism is in place to monitor how risk management is applied.
Staff complement	There are no dedicated resources allocated to risk management.	While there is a risk management team, its staffing level is being developed.	The risk management function has sufficient resources, and risk management accountabilities and responsibilities have been assigned at appropriate levels.	There is sufficient staff. In addition, the team is occasionally reinforced through independent experts from business areas or other central banks.
Staff expertise	No staff with basic knowledge of risk management principles.	Key officers have an understanding of the need to manage risks effectively and have a grasp of the key concepts involved. Staff assigned to risk management have no risk-related background (learning on the job). Only key staff are provided training and guidance material to assist in the management of risks.	There is an established core of staff with responsibility for risk management who have the skills and knowledge to manage risk effectively. Staff's skills and knowledge are supplemented by the provision of appropriate guidance and training.	All staff with responsibility for risk management have relevant skills and knowledge to manage risk effectively, and regular training (e.g., specialized training, conferences, seminars, forums) is attended to enhance their skills. There is ongoing specialist risk management support available for staff. Communication of the need for risk awareness and the provision of risk management training is bank-wide and all staff are encouraged and supported to take responsibility for effective risk management within their function/department. Initiatives are in place to train relevant staff from business areas on risk management issues.

Maturity Stages				
	Informal	**Developing**	**Implementing**	**Optimized**
Middle Office Function	The Bank has no middle office.	Very limited middle office function, possibly merged with front or back office. No clear mandate nor reporting to oversight bodies. The function lacks tools and staff skills to conduct its role.	Middle Office has a separate team with clear mandate but reporting lines to senior management only. Also, periodic reporting (scope and frequency) could be improved.	Middle Office has a separate team with enough resources and clear mandate working autonomously from front and back offices. The team has adequate reporting lines to oversight bodies (i.e., Board and Investment Committee). All relevant reports are in place and issued periodically.
Risk Management Process, Tools, & Methodologies				
Identification				
Structured approach	No structured risk identification.	The central bank does not have a risk management process (systematic approach) designed to identify all potential risks.	The central bank has a risk management process designed to identify all potential risks, only known by staff of the risk management unit / team.	Appropriate tools and techniques (e.g., process documentation, scenario analysis, risk and control self-assessments workshops) to identify potential risks. These are clearly documented and understood by all relevant participants, inside and outside of the risk management unit / team.
Risk universe	No formal risk universe in place.	Only common risks are considered in the framework (for example operational risks related to core areas such as currency, payment systems, banking operations, asset management).	In addition to common risks, the risk universe includes other horizontal / transversal risks (affecting multiple business areas and process such as system failure, power shortage, etc.).	The risk universe is expanded to include risks stemming from projects. The risk universe is updated at an appropriate frequency.
Risk incidents register	No risk incidents register in place.	Informal/ad-hoc documentation of risk incidents, but no standardized templates or procedures of incident reporting.	A main risk register is in place covering all functions/departments. Capturing risk incidents is formalized in dedicated templates (registers and catalogues). In addition to risk registers being updated periodically, there is also an established process to help ensure that significant changes are captured and communicated timely throughout the central bank and steps are taken to mitigate them. However, incident reporting is not exhaustive.	Institutional/structured process to report risk incidents. Dedicated risk management software. Formal catalogue of risks, root causes and impact. Quantification per risk. Reports obtained from the tools. In addition to annual updates of risk registers, the central bank also considers "near misses". The risk culture is supportive of incidents reporting across all business areas/functions within the bank in a timely manner.

Maturity Stages				
	Informal	**Developing**	**Implementing**	**Optimized**
Assessment & Measurement				
Assessment method	No clear method of assessment is in place.	Risk assessment processes are being developed but their application is inconsistent across the central bank. Only qualitative approach (expert opinion) of assessment is in place for operational risk management.	A range of different methodologies are used in key areas of the central bank (i.e., reserves management, banking operations, currency operations, payment systems), but all identify risks in a structured manner, taking into account both the likelihood and potential impact aspects. Both quantitative and qualitative methods are used to analyze and evaluate risks. No tools/checks are in place to ensure that risk assessment is consistent across departments/functions (e.g., assessment of potential impacts of similar risks differ).	Risk assessment processes are integrated as part of all business processes. Risk assessments are conducted through end-to-end processes supported by a risk management system. Both quantitative and qualitative methods are used according to a defined methodology. Checks are in place to ensure that risk assessment is consistent across departments/functions.
Risk heat map	There is no risk heat map.	There is a risk matrix (or similar) that illustrates the impact/relevance/importance of each risk. However, the values/parameters used for risk assessment are ill defined and do not allow for prioritization of the risks and respective action plans (e.g., the matrix is showing too many high risks).	The risk matrix (or similar) is clearly documented and allows for prioritization of risks and action plans. However, the risk matrix is only understood and used by the risk management unit/team.	There is a risk matrix known by the whole bank and some additional information (e.g. dashboard) to reflect also other risk related information, e.g. status of risk mitigation measures (delayed, on time).
Risk quantification	No quantification	VaR calculation and quantitative metrics only for financial risks.	VaR calculation and quantitative metrics for financial and operational risks (the latter only for information purposes).	Quantification is applied on all risk types to better assess their financial impacts and provide for adequate buffers.
Risk Responses				
Risk treatment / Action plans	No action plans.	Risk treatments/mitigation measures have been identified for some risks, but not converted into formal action plans and no mechanism to ensure their implementation and for assessing their effectiveness.	Risk treatment/mitigation plans include alternative courses of action and cost/benefit analyses of treatments. Action plans are recorded and there is a formal process of monitoring treatments. No reporting to oversight bodies.	Responses to risks are commensurate to the level of risk, including risk appetite and tolerance levels defined across the central bank. There is a formal register of action plans (portfolio approach), monitored regularly to ensure that risk treatments focus on highest

Maturity Stages				
	Informal	**Developing**	**Implementing**	**Optimized**
				priorities, remain effective, and reported to senior management and oversight bodies. Risk treatment options that can address multiple risks are considered to avoid duplication and unnecessary cost.
Cost/Benefit analysis	No cost/benefit analysis is performed to analyze mitigation measures.	The evaluation is subjective, based on the experience of the risk owners.	A clear cost/benefit assessment is applied for some mitigation measures.	A cost-benefit analysis is applied for all risk treatments.
Accountability framework	No one is accountable for risk treatment.	By default, managers are accountable for risks and are responsible for risk treatments in their areas of responsibility.	Managers are accountable for risks and responsible for action plans in their respective areas/departments.	The ownership of risk treatments has been appropriately assigned; all staff involved are aware of their responsibilities and resource requirements are clear, including contingencies. Reporting requirements to senior management and the oversight body are also established. Managers' performance appraisals take into account the implementation of risk action plans.
Contingency plans	The central bank is not aware of its major risks, and therefore there are no contingency plans.	The central bank is aware of its major risks, but has no specific contingency plans to address those risks that might materialize despite the controls in place.	The central bank has contingency plans for its major risks.	The central bank has reliable contingency arrangements in place; all scenarios and potential impacts have been analyzed and optimized contingency plans have been established.
Business continuity	Business continuity function is not integrated with risk management.	Risk management is informed about business continuity work and vice versa, but there is no formal coordination between the functions.	Both functions cooperate occasionally (for example, they share a common list of processes and business continuity uses risk management information to update the list of critical processes).	Risk management and business continuity are fully integrated. They share tools and contribute to each other planning by providing inputs and suggestions. Teams meet regularly, and risk management participates in business continuity drills.Both functions participate in initiatives of common interest, such as cyber security.

Maturity Stages				
	Informal	**Developing**	**Implementing**	**Optimized**
Monitoring & Reporting				
Reporting mechanism	No risk reporting in place.	There is limited risk management reporting (performed on an ad-hoc basis). Key staff are aware of risk management developments; however this information is not disseminated to a wider audience within the central bank. No risk performance monitoring reports are provided to senior management (Board and executive management).	Risk is a standing agenda item for senior management meetings. Risk management reporting has been developed with regular reports going to senior management and relevant committees.	Risk management reporting is embedded into the overall governance framework of the central bank. Information derived from the application of risk management is relevant and available at appropriate levels and times. In particular, risk management communications to the Board and its committees are consistent with agreed-upon protocol, at the appropriate level of details, and timely. Performance measurements (KRIs), reporting requirements, and escalation processes are in place and working effectively. Periodic and formal meetings with dedicated risk management oversight body with clear agenda and follow up of decisions taken.
Risk management annual report	No annual report is prepared.	The oversight body is informed on ad-hoc basis.	The oversight body receives a standardized annual report with all relevant information on it. The report is exclusive for the risk management team/unit.	The oversight body receives an annual report with all relevant information and risk analysis. The report is prepared jointly with other relevant functions / departments (e.g., security, IT).
Evolution and continuous improvement				
Review of risk management practices				
	None.	Changes to risk management processes are introduced to address shortcomings and/or significant shifts in the control environment.	The central bank has a periodic review (self-assessment) of its risk management processes and improvements are made accordingly. Passive participation in international risk management initiatives (e.g., seminars, conferences, training).	All aspects of the risk management framework are reviewed at least annually, with improvements made to help ensure that it remains fit for purpose. There is a standard and consistent process for the evaluation of risk management and alignment with leading practices, including the risk management policy. Active participation in international initiatives (e.g., seminars,

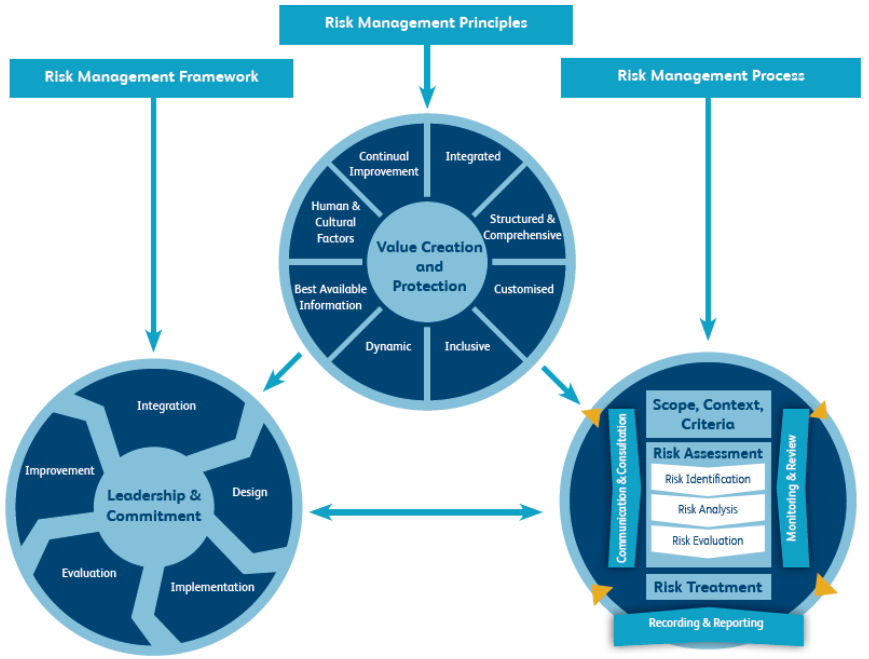
Maturity Stages				
	Informal	**Developing**	**Implementing**	**Optimized**
				conferences, training) for knowledge sharing in risk management. The adequacy and effectiveness of risk management is periodically reviewed by Internal Audit. Internal Audit provides useful insights into the progress of risk management within the central bank. Its outputs are implemented to improve the function and are subject to periodic review by the Audit Committee and the Board Risk Committee.

Annex II. Overview of ISO 31000 and COSO ERM

ISO 31000

ISO 31000 was originally published by the *International Standards Organization* (ISO) in 2009 and an updated version was published in February 2018. A key feature of this international standard is integrating the management of risk into a strategic and operational management system, and expanding the responsibility for risk management to a broader group of risk owners across an organization. ISO 31000 suggests that effective risk management is characterized by principles, framework and process as depicted in the figure below, and will depend on its integration into all aspects of the organization:[20]

Figure 2. Principles, Framework and Risk Management Process from ISO 31000



Source: Reproduced from *ISO 31000: 2018 Risk Management – Guidelines*

While the revised standard is very similar to the original version, key changes include: (i) risk management is no longer an activity conducted in silo, but rather integral part of high-level and operational decision-making; (ii) risk management is iterative and should be continuously improving to adapt to external and internal changes.

[20] *A Risk Practitioners Guide to ISO 31000: 2018* – Institute of Risk Management (IRM)

COSO/ERM

Probably the most widely applied Enterprise Risk Management (ERM) framework-the COSO ERM framework- was first developed by the US Committee of Sponsoring Organizations of the Treadway Commission (COSO) in 2004. It was defined as "a process, affected by the entity's board of directors, management, and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within the risk appetite, to provide reasonable assurance regarding the achievement of objectives".

The framework was updated in 2017 with the aim of improving organizational performance through better integration of strategy, risk, control and governance. It clarifies the importance of enterprise risk management in strategic planning and emphasizes embedding ERM throughout an organization, as risk influences strategy and performance across all functions. The COSO Enterprise Risk Management Framework, as shown below, is a set of principles organized into five interrelated components.[21]

Figure 3. Enterprise Risk Management

Source: Reproduced from *COSO – Enterprise Risk Management – Integrating with Strategy and Performance*

The two frameworks touch on similar aspects of the risk management process. While there are nuances between ISO 31000 and COSO ERM, the basis of both frameworks is essentially the identification of high-level objectives that are used as the standards for evaluating the effectiveness and efficiency of risk management. Both COSO ERM and ISO 31000, because of their maturity, their holistic approach and their similarities in methodology, can help organizations to realize the potential benefits connected with the application of a generic risk management standard.

[21] Enterprise Risk Management – Integrating with Strategy and Performance, June 2017 (*Committee of Sponsoring Organizations of the Treadway Commission COSO*)

REFERENCES

A Risk Practitioners Guide to ISO 31000: 2018 – Review of the 2018 version of the ISO 31000 risk management guidelines and commentary on the use of this standard by risk professionals (*Institute of Risk Management- irm*).

ISO 31000: 2018 Risk Management – Guidelines (*International Standards Organization ISO*)

Enterprise Risk Management – Integrating Strategy and Performance, June 2017 (*Committee of Sponsoring Organization of the Treadway Comission COSO*)