ENTERPRISE RISK MANAGEMENT GUIDANCE NOTES

BANK SUPERVISION DEPARTMENT

Date Issued: 22 June, 2023

TABLE OF CONTENTS

INTRODUCTION

1. The Central Bank requires that all Supervised Financial Institutions ("SFIs") implement an appropriate Enterprise-wide Risk Management ("ERM") framework. These Guidance Notes sets out the minimum standard that the Central Bank expects SFIs to adopt for evaluating risk, identifying material and emerging problems, and prompt corrective action to safeguard their financial safety and soundness.

2. All SFIs are required to adhere to the Central Bank's licensing and prudential requirements, ongoing supervisory programmes, required regulatory reporting, and are subject to periodic onsite inspections. SFIs are also expected to conduct their affairs in conformity with all other Bahamian legal requirements and international best practices.

3. These Guidance Notes serve as a general guide to ERM. Nothing herein prevents or limits the Central Bank from taking any course of action it deems necessary, for the protection and strengthening of the financial system in The Bahamas.

APPLICABILITY

4. These Guidance Notes apply to SFIs incorporated in The Bahamas, inclusive of co-operative credit unions, but does not apply to nominee trust companies.[1]

5. The Central Bank endorses and has incorporated into its Supervisory Review Process, the Basel Committee's "*Risk Management*" principles at www.bis.org and the Financial Stability Board's "*Principles of an Effective Risk Appetite Framework*". The Central Bank encourages SFIs to read these Guidance Notes in conjunction with the full Basel document, as well as:

   (a) The Bahamas Capital Regulations, 2022 ("the Capital Regulations");
   (b) Corporate Governance Guidelines;
   (c) Guidelines for the Internal Capital Adequacy Assessment Process for Licensees ("ICAAP");
   (d) Guidelines for the Management of Country Risk;
   (e) Guidelines for the Management of Credit Risk;
   (f) Guidelines for the Management of Interest Rate Risk;
   (g) Guidelines for the Management of Liquidity Risk;
   (h) Guidelines for the Management of Operational Risk;
   (i) Guidelines for the Management of Technology Risk;
   (j) Guidelines on Minimum Standards for the Outsourcing of Material Functions;
   (k) Guidelines for the Management of Market Risk; and
   (l) Recovery Planning Guidelines.

[1] Although nominee trust companies are exempt from these Guidance Notes, it is the Central Bank's expectation that the risk assessments of their parent companies will include their enterprise risks.

DEFINITIONS

6. In these Guidance Notes –

"Banking Group" includes the holding company, the bank and its offices, subsidiaries, affiliates and joint ventures, both domestic and foreign;

"Central Bank" means the Central Bank of The Bahamas established pursuant to Section 3 of the Central Bank of the Bahamas Act, 2020 (No. 24 of 2020);

"Enterprise Risk Management" or **"ERM"** means a process that involves identifying, measuring, monitoring, reporting, and responding to risks across a SFI that is aligned with its objectives and risk appetite;

"Fiduciary risk" means the risk to earnings and capital resulting from a breach of duty in advising on, or in holding, administering, managing or investing the assets of a client or other third party;

"Inherent risk" means the risk associated with any current or future process or activity before the implementation of risk mitigating mechanisms and control;

"Internal controls" means a process, designed to provide reasonable assurance regarding the achievement of objectives relating to operations, reporting, and compliance;

"Monitoring" means the continual checking, supervising, critically observing or determining the status in order to identify change from the performance level required or expected;

"Residual risk" means the risk that remains after risk management controls are applied to the inherent risk;

"Risk" means the possibility that an event of a given impact will occur, adversely affecting the achievement of objectives;

"Risk appetite" refers to the aggregate level and types of risk a SFI is willing to assume to achieve its strategic objectives and business plans;

"Risk appetite statement" means the written form of the aggregate level and types of risk that a SFI is willing to accept, or to avoid, in order to achieve its business objectives;

"Risk concentration" means any single exposure or group of similar exposures (i.e. to the same borrower/counterparty, geographic area, industry etc.) with the potential to produce losses large enough to threaten a bank's creditworthiness or ability to maintain its core operations or a material change in a bank's risk profile;

"Risk culture" means a bank's norms, attitudes and behaviors related to risk awareness, risk-taking and risk management, and controls that shape decisions on risks. Risk culture influences the decisions of management and employees during the day-to-day activities and has an impact on the risks they assume;

"Risk owners" means the first line decision maker(s) with the accountability, authority and responsibility to manage risks in their span of control;

"Risk profile" means a composite view of the risk assumed at a particular level of the SFI, or aspect of the business, that positions management to consider the types, severity and interdependencies of risks and how they may affect performance relative to the strategy and objectives;

"Risk tolerance" is the variation around the prescribed risk appetite that the SFI is willing to take;

"Settlement risk" means the risk to earnings or capital arising when the completion or settlement of a financial transaction fails to take place as expected. Settlement risk is often associated with credit risk, liquidity risk, market risk, operational risk and reputation risk;

"Strategic risk" means the current and prospective impact on earnings or capital arising from faulty business strategies and decisions, improper implementation of strategies and decisions, or lack of response to industry changes;

"Supervised Financial Institution" or **"SFI"** means any licensed bank, bank and trust company, and co-operative credit union regulated by the Central Bank; and

"Technology risk" means the risk to earnings or capital arising from inadequate, obsolete, or mismanaged technology or from a failure or interruption in technology caused by events within or outside the SFI.

RISK MANAGEMENT

7. Risk management processes should be an integral part of management and decision-making, and integrated into the structure, operations and processes of the SFI. An effective risk management framework, that is proportionate with the size, complexity, risks, and business model of a SFI's operations, must be in place to help ensure that risks are well managed within the SFI's risk appetite and that the necessary systems and controls are in place to achieve the intended results.

8. SFIs should have a comprehensive risk management framework, including effective Board and senior management oversight to identify, measure, evaluate, monitor, report and control or mitigate all risks on a timely basis and to assess the adequacy of their capital and liquidity in relation to their risk profile and market and macroeconomic conditions. This extends to the development and review of contingency arrangements, including recovery plans, which take into account the specific circumstances of the SFI on a consolidated basis. SFIs that are a part of a banking group may rely on the risk management function within the group, where the risk management function satisfies the criteria set out below.

9. Depending on the specific types of businesses conducted by individual SFIs, such risks[2] may include at a minimum:

   (a) credit risk;
   (b) compliance risk;
   (c) fiduciary risk;
   (d) interest–rate risk;
   (e) legal risk;
   (f) liquidity risk;
   (g) market risk;
   (h) operational risk;
   (i) reputation risk;
   (j) settlement risk;
   (k) technology risk; and
   (l) any other risk[3] that is identified as material to the particular business of a SFI.

[2] These risks are generally associated with the businesses conducted by banks and may not always be applicable to the activities of trust companies.
[3] Other risks can include country risk, transfer risk, strategic risk, cyber risk and risk associated with digital assets.

KEY ELEMENTS OF AN EFFECTIVE RISK MANAGEMENT FRAMEWORK

10. To ensure an effective risk management framework, SFIs should have in place a robust risk governance framework, which outlines and defines the responsibilities of the Board and senior management, the different business lines and the respective risk owners. The risk governance framework should outline appropriate notification and escalation channels to the board and senior management, action plans to remediate any gaps, and potential disciplinary actions for excessive risk taking.

11. SFIs should ensure that the risk management framework has the following features:

    (a) a Board-approved risk appetite statement;
    (b) active board and senior management oversight;
    (c) appropriate policies, procedures and other mechanisms to manage risks;
    (d) a comprehensive risk management lifecycle as specified in these Guidance Notes;
    (e) a risk reporting management information systems ("MIS") at the business line and institution-wide level; and
    (f) comprehensive internal controls.

Risk Appetite Statement

12. SFIs should develop a Board approved risk appetite statement that includes qualitative statements as well as quantitative measures expressed relative to earnings, capital, risk measures, liquidity and other relevant measures as appropriate including more difficult to quantify risks such as reputational risk.

13. Risk appetite statements help to make risk-informed decisions with regard to the allocation of resources, management controls, and potential consequences or impacts to other parts of the SFI, and can reduce surprises and unexpected losses. Therefore, SFIs are expected to develop a risk appetite statement that clearly articulates the tone of the SFI and set clear boundaries and expectations.

14. At a minimum an effective risk appetite statement should:

    (a) include key background information and assumptions of the SFI's strategic and business plans at the time they were approved;
    (b) be linked to the SFI's short- and long-term strategic goals, capital and financial plans, as well as compensation programs;
    (c) establish the amount of risk the SFI is prepared to accept in pursuit of its strategic objectives and business plan, taking into account the interests of its customers and the fiduciary duty to shareholders, as well as capital and other regulatory requirements;
    (d) determine for each material risk and overall the maximum level of risk that the SFI is willing to operate within, based on its overall risk appetite, risk tolerance, and risk profile; and
    (e) include quantitative measures and qualitative statements that can be aggregated and disaggregated at the business line level, entity level, and group level.

Risk Governance

15. Risk governance refers to the formal arrangements that enables the Board and senior management of a SFI to establish sound business strategy, articulate and monitor adherence to risk appetite and risk tolerance, and identify, measure, manage and control risks.

16. Effective management engages employees at all levels and allows risks to be escalated to the appropriate level of decision making. The responsibilities among the different business lines should be defined in such a way that there are three lines of defence which are independent of each other.

17. The risk roles and responsibilities are distributed by activities between ***the first line*** risk decision makers who own and manage risk as part of the day-to-day work, ***the second line*** risk managers and compliance functions who monitor risk controls, set standards and define overall risk appetite, and ***the third line*** independent internal auditors.

Role of the Board of Directors

18. The Board of Directors and senior management should be aware of the major aspects of the SFI's risks as they are ultimately responsible and accountable for the overall risk profile of the business.

19. The Board should:

    (a) approve a written risk management framework strategy which addresses all risks that are likely to be exposed based on the business activities of the operation, including outsourced business or with respect to new products/services to be launched;
    (b) oversee the implementation of key policies and procedures that are consistent with the SFI's risk appetite, risk profile and capital strength (i.e. capital adequacy assessment process, capital and liquidity plans, compliance policies and obligations, and the internal control system);
    (c) establish appropriate risk tolerance limits on the SFI's activities which are consistent with its risk taking appetite and capacity that are understood by, and regularly communicated to relevant staff;
    (d) clearly identify managerial responsibilities and controls, designed to ensure that the policies and procedures are adhered to at all times;
    (e) review the risk management framework annually or more frequently, when there is a significant change in their risk environment to ensure that it remains adequate and appropriate under changing business and market conditions; and
    (f) establish both top-down board leadership and bottom-up involvement of management at all levels, embedded and understood across the SFI.

Role of Senior Management

20. Senior Management should:

    (a) develop detailed policies, procedures and limits for managing different aspects of risk arising from the various business lines/activities, based on the risk management strategies provided by the Board;
    (b) remain informed by the first line of defence, on an on-going basis about risks, financial markets, risk practices as the SFI's activities evolve and report all relevant information to the Board;

(c) establish and communicate a strong awareness of and need for effective internal controls;
(d) manage risk in a manner that clearly indicates where in the SFI, each segment of risk concentration resides and have credible risk mitigation strategies in place that have senior management approval; and
(e) ensure that management and staff responsible for risk management and control functions understand the risk facing the SFI's pursuit of the objectives; implementing appropriate programmes to recruit, train and retain employees with suitable skills and expertise.

Risk Management Policies, Procedures and Limits

21. A SFI's policies, procedures and limits should:

(a) provide for adequate and timely identification, measurement, monitoring, control and mitigation of the risks posed by its lending, investing, trading, securitisation, off-balance sheet, fiduciary and other significant activities at the business line and institution-wide levels;
(b) ensure that the economic substance of its risk exposures, including reputational risk and valuation uncertainty, are fully recognised and incorporated into its risk management processes;
(c) be consistent with its stated goals and objectives, as well as its overall financial strength;
(d) clearly delineate accountability and lines of authority across its various business activities, and ensure there is a clear separation between business lines and the risk function;
(e) escalate and address breaches of internal position limits;
(f) provide for the review of new businesses and products by bringing together all relevant risk management, control and business lines to ensure that it is able to manage and control the activity prior to it being initiated; and
(g) include a schedule and process for reviewing the policies, procedures and limits and for updating them as appropriate.

22. The policies and procedures should be developed based on a comprehensive review of all business activities, and cover all material risks, both financial and non-financial associated with the SFI's activities. They should be prepared on an institution-wide basis and, where applicable, on a group-wide basis.

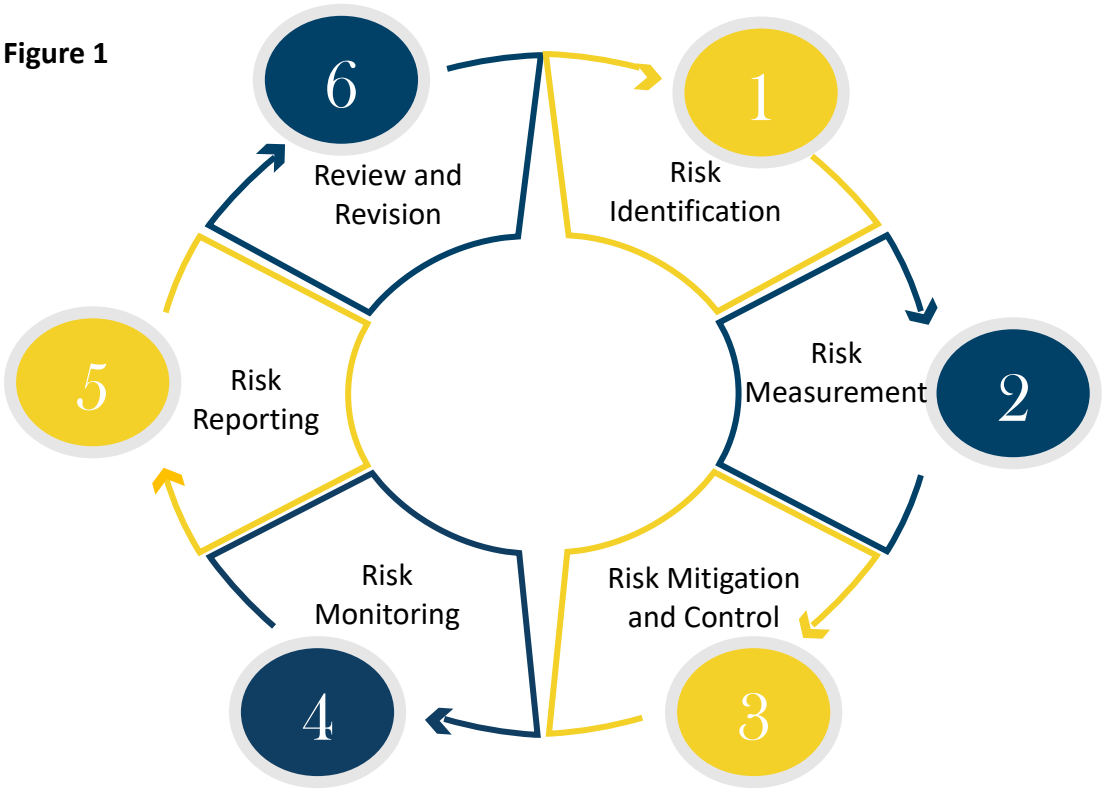
23. SFIs should set risk limits based on various levels (i.e. individual business lines, or the group as a whole) with a clearly documented methodology for allocating overall risk tolerance across each.

Risk Management Lifecycle

24. The risk management process is an ongoing cycle that is defined as a comprehensive and timely identification, measurement, mitigation, controlling, monitoring, and reporting of risks. The Board and senior management of the SFI should analyse its existing and prospective business, products and services to identify and measure the types and significance of the current and potential risks that must be managed and controlled, both individually and taken together.

25. The Board and management should develop and implement appropriate and prudent risk management policies and procedures and monitor their effectiveness through timely, accurate, relevant and complete information systems. Provision should also be made for appropriate action to deal with extraordinary events; i.e. contingency plans. This process is illustrated in Figure 1.

Figure 1



Step 1: Risk Identification

26. SFIs should consider all relevant information when identifying and assessing inherent risk. Risk concentrations should be analysed on both individual institutional level and consolidated basis, as an unmanaged concentration at a subsidiary bank may appear immaterial at the consolidated level, but can nonetheless threaten the viability of the subsidiary organisation. SFIs should also regularly identify and consider new developments or emerging risks that may impact their risk profile.

27. Risk concentrations can also arise through both direct and indirect exposures and should be taken into consideration when developing a list of risk factors. The purpose of the risk identification process is not to collect an exhaustive list of all risk factors within the SFI, but rather to identify the risks that are most relevant. A number of techniques are available for identifying risks and SFIs should consider the nature and type of the risk to determine the appropriate technique.

28. Depending on the number of individual risks identified, SFIs may structure the risk inventory/register by category to provide standardised descriptions and definitions for different risks. This allows similar risks to be grouped together (i.e. financial risks, customer risks, compliance risks etc.) and further defined into more detailed sub-categories as needed.

Step 2: Risk Measurement

29. After the risk identification is completed, the next step is to understand the materiality/severity of each risk to the achievement of the SFI's strategy and defined objectives, and to support the selection of the risk response. These measures should align with the nature, size, and complexity of the SFI and its risk appetite. Different thresholds may also be used at varying levels for which a risk is being assessed.

30. Measures may include:-

(a) the probability of the risk occurring – when assessing the likelihood, consideration is given to the future probability which may be informed by the frequency of occurrence in the past and validated by data gathered about the control environment from risk indicators, incidents and audit/evaluation or management/oversight issues. It can range from very unlikely to very likely; and
(b) the impact of the event – the severity or the range of possible effects associated with the risk. The impact of a risk may be positive or negative relative to the strategy or business objectives.

31. Risk identification and measurement should include both quantitative (i.e. score value/ percentage) and qualitative (i.e. low, medium, high) elements on an institution-wide risk level relative to the external operating environment. SFIs should also take special care when considering and evaluating risk which may be more difficult to quantify (i.e. reputation risk).

32. The accuracy and reliability of an adopted risk measurement technique should be verified against actual results through regular back-testing. The measurement technique should also be subject to periodic updates to reflect changing market conditions.

Step 3: Risk Mitigation and Control

33. Once risks have been identified and measured for materiality, management selects and deploys a risk response. Risk response strategy types are summarised below:-

(a) avoidance – an activity seeking to completely eliminate risk or uncertainty by deflecting the threat as much as possible. Choosing avoidance suggests that management has not been able to identify a response that would reduce the risk to an acceptable level of materiality;
(b) acceptance – risk is accepted without the need for any further mitigating measures. Choosing acceptance usually applies when the risk is within appetite or sometimes also when a risk is out of appetite but there is no feasible mitigation;
(c) transfer – mitigating action is taken to reduce the probability and/or potential impact of the risk bypassing ownership and/or liability to a third party (i.e. outsourcing arrangements); and
(d) mitigation – reducing the probability and/or severity of the risk below an acceptable threshold. This involves recognizing residual risks and developing responses to control and monitor them.

34. As part of the risk assessment, SFIs should identify the inherent risk levels, mitigating controls, and residual risk levels. Risk is managed at residual risk levels, therefore, inherent risk rating provides the probability and impact of a risk materialising without the presence of any internal controls to prevent, detect or correct a risk event. The mitigating controls will alter the severity of the risk resulting in the reduction of the impact and/or probability of the associated

risk, known as the residual risk. Where the level of residual risk exceeds a SFI's risk tolerance, or where its mitigation measures do not adequately mitigate high risks, the strength of mitigation measures should be increased.

35. The Central Bank recognises that risk in any business operation is unavoidable, but management is required to make risk-informed decisions to balance risk and opportunities, and in certain instances, offset one type of risk against another to minimise overall exposure to risk. SFIs should establish and communicate risk tolerance through policies, standards and procedures that define responsibility and authority.

Step 4: Risk Monitoring

36. SFIs are expected to adopt a system for measuring the performance of their business lines on a risk-adjusted basis to enable them to compare the financial performance of individual business lines, taking into account the risks associated with their activities and any breaches of risk limits or other risk management measures. This ensures that business units are not rewarded for taking on excessive risks.

37. To enable efficient allocation of resources to individual business lines and to provide these units with incentives for controlling the risks generated from their activities, the performance measurement system used should be able to comprehensively measure the risks associated with the individual business activities. Management information systems should be able to attribute risk and earnings to their appropriate sources and to measure earnings against resources allocated to the activity, after adjusting for various risks.

Step 5: Risk Reporting

38. Effective risk management requires a continual process of capturing and sharing risk information that flows top down, down up and across the three lines of defence. Risk reporting is therefore required at all levels of the SFI, based around risk categories and supported by relevant risk data within the framework.

39. Reporting is an integral part of the SFI's governance and should enhance the quality of dialogue with stakeholders and support senior management in meeting their responsibilities. What information is available to management, what information systems and technology are in use for capturing that information, and what the costs are of obtaining that information is imperative when identifying how information supports the enterprise risk management practices. SFIs are also expected to measure and monitor the level of completeness to ensure that any gaps do not critically affect their ability to manage their risks. Exceptions to data completeness should be identified and explained.

Step 6: Review and Revision

40. A SFI ought to ensure the compliance and effectiveness of the risk management framework is subject to review by internal and/or external audit at least annually or more frequently as required. The scope of the review must take into consideration the nature, size, complexity of the SFI's business activities, the extent of any change to its operations or risk appetite, and any changes to the external environment in which the institution operates.

41. If performance does not fall within the acceptable range prescribed (i.e. a change in risk profile) SFIs may need to review and revise their risk tolerance, how risks are prioritised, risk

response, and risk appetite etc. The extent of any corrective actions must align with the magnitude of the deviation in performance, the importance of the business objective, and the costs and benefits associated with altering risk responses.

MANAGEMENT INFORMATION SYSTEM (MIS)

42. SFIs should establish and maintain a management information system with adequate technological support and processing capacity to effectively capture, aggregate and report on the risks of business activities within the SFI. The risk data aggregation and risk reporting framework should be reviewed annually or more frequently, if there is a significant change in their risk environment and approved by the Board and senior management.

43. The key elements necessary for the aggregation of risks are an appropriate infrastructure and MIS that:-

(a) allow for the aggregation of exposures and risk measures across business lines; and
(b) support customised identification of concentrations and emerging risks.

44. The level of sophistication of the risk management information system should be commensurate with the nature, scale and complexity of the SFI's business activities. The MIS should support decision-making at different levels and enable early identification of emerging risks. It should be capable of:

(a) accurately and reliably capturing, aggregating and reporting risk data in a timely manner, not only in normal times but also in times of stress;
(b) capturing, aggregating and reporting risk data on all sources of relevant risks;
(c) supporting customised identification, aggregation and reporting of risks (e.g. based on individual or a set of closely related risk drivers) to meet requests of the Central Bank, the Board, senior management and stakeholders;
(d) incorporating changes arising from regulatory requirements and new business developments as and when necessary; and
(e) supporting a broad range of risk management analysis, including but not limited to:
    - incorporating multiple perspectives of any particular risk exposure to account for changes in uncertainties in risk measurement;
    - incorporating any risk-mitigating actions to be carried out on an institution-wide basis while taking into account various related basis risks;
    - reporting excesses in limits and policy exceptions, and alerting management of risk exposures approaching pre-set limits;
    - facilitating the allocation of capital charges to business activities according to the level of risk-taking;
    - conducting variance analysis against annual budget or business targets, and calculating risk-adjusted performance; and
    - providing adequate system support for fair valuing of exposures.

45. Risk management reports should communicate information in a clear and concise manner, yet be comprehensive enough to be useful for informed decision-making and risk assessment. Frequency, timeliness, contents, granularity, distribution and level of confidentiality of risk management reports should be appropriate for the needs of recipients. While SFIs should determine risk reporting requirements that are appropriate for their own business risk profiles, at a minimum, the reports should cover all material risk areas and provide information in respect of risk concentrations, adherence to risk appetite and risk tolerances and forward-looking assessments of risk.

46. There should be proper control, validation and reconciliation processes in place to ensure the accuracy of risk management reports, and relevant processes should be documented with appropriate explanation. For instance, it is expected that risk data aggregation should occur on a largely automated basis. There should be automated and manual checks, including validation rules to help verify data inputs and calculations.

47. To remain effective, there should be processes to identify, rectify and alert senior management (where appropriate) of any incompleteness, exception, limitation and weakness of the SFI's risk management information system in capturing, aggregating and reporting of risks. The system should also be subject to regular review and enhancement. Moreover, the capabilities of the SFI's risk management system should be considered by the Board and senior management as part of any approval process for new initiatives and a clear timeframe should be set for making any required upgrading or adjustment.

INTERNAL CONTROLS

48. A critical element to support an effective risk management framework is the existence of a sound internal control system. Such a system helps to ensure that the SFI will comply with laws and regulations as well as policies, plans, internal rules and procedures, and decrease the risk of unexpected losses or damages to the SFI's reputation.

49. A SFI's internal control system should, at a minimum, cover the following:

(a) high level controls, including clear delegation of authority, written policies and procedures, separation of critical functions;
(b) controls relating to major functional areas, such controls should include segregation of duties, authorisation and approval, tolerance monitoring, physical access controls, etc.;
(c) controls relating to financial accounting, annual budgeting, management reporting and compilation of prudential returns to the regulators;
(d) controls relating to information technology;
(e) controls relating to outsourced activities, where applicable; and
(f) controls relating to compliance with statutory and regulatory requirements.

50. An effective internal control system requires a strong control environment to which the Board and senior management provide their full support, and an internal audit function evaluates its performance on a regular basis.

51. There should be an effective and comprehensive internal audit of the internal control system carried out by operationally independent, appropriately trained and competent staff. The internal audit function, as part of the monitoring of the system of internal controls, should report directly to the Board or its audit committee.

INTERNAL AUDIT

52. The internal audit function is an important part of the ongoing monitoring of the system of internal controls because it provides an independent assessment of the adequacy of, and compliance with, the established policies and procedures.

53. It is critical that the internal audit function is independent from the day-to-day functioning of the SFI and that it has access to all activities conducted by the SFI, including at its branches and subsidiaries. In fulfilling its responsibilities relating to a SFI's risk management, the internal audit function should among other things, (on a group basis and on the basis of individual business lines and legal entities) assess and report to the Board or its audit committee periodically on whether:

    (a) the SFI's risk governance arrangements and risk appetite framework are effective, both in their design and operation (including the linkages to the SFI's risk culture, strategic and business planning, remuneration and decision-making processes);
    (b) breaches of risk limits are being appropriately identified, escalated and reported;
    (c) the SFI's risk measurement techniques and risk management information system and related reporting are effective; and
    (d) the SFI's internal control system is effective.

54. Additionally, the compliance function plays an important role with respect to a sound risk management framework, but should not be regarded as a substitute for regular and adequate internal audit coverage. The work of the compliance function should be subject to periodic reviews by the internal audit function.

DISCLOSURE

55. The Central Bank encourages all SFIs to disclose relevant information regarding their enterprise risk management framework to allow stakeholders to determine whether the SFI identifies, assesses, monitors and controls/mitigates operational risk effectively. Disclosures should be commensurate with the size, risk profile and complexity of a SFI's operations.

REPORTING REQUIREMENTS

56. The Central Bank, as part of its ongoing supervisory responsibilities, will assess the degree of SFIs' compliance with the principles set forth in these Guidance Notes, taking into account the nature, size, risk profile and complexity of the SFI's activities.

57. SFIs are required to submit to the Central Bank, their board approved enterprise-wide risk assessment signed by the Chairman of the Board and the Chairman of the Risk Management Committee or the Audit Committee, via the ORIMS Portal. **Appendix 1** provides a summary of the key information that should be included in the submitted ERM risk assessment. The list is not exhaustive and is merely a guide of the minimum expectation of the Central Bank.

58. SFIs must notify the Central Bank no later than ten business days after it becomes aware of any significant breaches, or material deviation from their risk management framework. The report should include a description of the cause/circumstance and the steps taken, or

proposed to be taken to remedy the problem. Further, SFIs are required to provide additional information upon request.

59. Where a SFI conducts business in a jurisdiction outside of The Bahamas, it must notify the Central Bank not more than ten business days, after it becomes aware that its right to conduct business in that jurisdiction has been materially affected by the laws of that jurisdiction or its right to conduct business has ceased.

60. The Central Bank reserves the right to require a SFI to amend its enterprise risk management framework where the Central Bank considers that the framework does not adequately address or cover all of the SFI's key risks.

APPENDIX 1

Key information to include in the Enterprise Risk Assessment

	Summary Description
Executive Summary	▪ Brief description of the report that include: o The immediate and ultimate parent body(ies); o its nature of business/corporate structure; o the country where it operates in; and o whether the entity is registered to operate in any other jurisdiction; ▪ Description of entities that are excluded from the report and the reason for their exclusion.
Risk Management Framework Overview	▪ The objectives and principles of the risk management framework; ▪ The risk taxonomy (a dashboard can be used); ▪ The key risks that affect the financial strength of the SFI; and ▪ The basis of preparation and the sources that comprise the report.
Risk Governance	▪ Identify the departments that drive the management of risk; ▪ Define the risk culture; ▪ Incorporate each line of defence; ▪ The risk committees involved and the responsibilities; ▪ Include a summary of the key risk management policies and the effectiveness of these policies; and ▪ All internal controls.
Risk Appetite Statement	▪ Determine the broad category (i.e. financial risk, strategy risk) and sub-category (i.e. credit risk, legal risk) for each risk; ▪ Define the risk tolerance (aligned with the business strategic goals) for each risk and the metric used for the assessment; and ▪ A limit/threshold should be determined at intervals for each risk.
Risk Identification	▪ Each risk is identified and assessed based on its probability and impact; ▪ The breakdown should include: o Risk Category; o Risk Sub-category; o Description of Risk Elements; o Key Inherent Risk; and o Inherent Risk Score; ▪ The information provided in the risk appetite section can be used.
Risk Measurement	▪ The impact and probability defined according to each risk;

<table>
<tr><th></th><th>Summary Description</th></tr>
<tr><td></td><td>

A probability scale should be a uniformed numerical scale:

An example of a uniform numerical scale - each interval is defined, scored and an explanation provided for each (i.e. low (score 1) – the chance of the risk occurring is on an exceptional basis; occurrence over 10 years):

<table>
<tr><th>Scale</th><th>Probability</th><th>Score</th></tr>
<tr><td>Low</td><td>Remote</td><td>1</td></tr>
<tr><td>Medium Low</td><td>Unlikely</td><td>2</td></tr>
<tr><td>Medium</td><td>Possible</td><td>3</td></tr>
<tr><td>Medium High</td><td>Likely</td><td>4</td></tr>
<tr><td>High</td><td>Almost Certain</td><td>5</td></tr>
</table>

An impact scale should be used:

An example of a uniform numerical scale - each interval defined and an explanation given for each (i.e. high (score 4) – significant consequences; widespread disruption of critical business functions):

<table>
<tr><th>Impact</th><th>Score</th></tr>
<tr><td>Low[4]</td><td>1 – Insignificant</td></tr>
<tr><td>Medium low[5]</td><td>2 - Minor</td></tr>
<tr><td>Medium high[6]</td><td>3 - Moderate</td></tr>
<tr><td>High[7]</td><td>4 - Significant</td></tr>
</table>

A heat map/table can be used to combine the probability and impact score; and
Additional illustration (i.e. pie chart, graphs) can be used to highlight the inherent risks of the SFI before risk mitigation.

</td></tr>
<tr><td>Risk Mitigation and Control</td><td>

The mitigation and control environment should be defined overall for each risk category/sub-category;
Information on the rationale or the tools/policies used for mitigation;
A description for the effectiveness of the mitigating controls for each risk profile can be used with a control rating i.e.:

</td></tr>
</table>

[4] Low inherent risk exists when there is a lower than average probability of a material loss due to exposure to, and uncertainty arising from, current and potential future events.

[5] Medium-low inherent risk exists when there is an average probability of a material loss due to exposure to, and uncertainty arising from, current and potential future events.

[6] Medium-high inherent risk exists when there is an above average probability of a material loss due to exposure to, and uncertainty arising from, current and potential future events.

[7] High inherent risk exists when there is a higher than above average probability of a material loss due to exposure to, and uncertainty arising from, current and potential future event.

	Summary Description
	<table><tr><th>Control Ratings</th></tr><tr><td>Strong</td></tr><tr><td>Satisfactory</td></tr><tr><td>Needs Improvement</td></tr><tr><td>Deficient</td></tr><tr><td>Critically Deficient</td></tr></table>
Risk Reporting	▪ The residual risk rating should be reported with an explanation; ▪ The overall aggregated score should be clearly summarized and reported; ▪ Corrective action plans should be reported with an explanation; and ▪ Limits/threshold that were breached should be explained and corrective actions provided.
Signatory Page	▪ The Chairman of the Board and the Chairman of the Risk Management Committee or the Audit Committee should review, approve and sign off on the risk assessment.