CENTRAL BANK of BELIZE

Basel II/III Implementation

Principles for the Management of Operational Risk

September 2021

Table of Contents

INTRODUCTION

Operational risk is defined as the risk of loss resulting from inadequate or failed internal processes, people and systems, or from external events. This definition includes legal risk but excludes strategic and reputational risk. Legal risk includes, but is not limited to, exposure to fines, penalties, or punitive damages resulting from supervisory actions, as well as private settlements.

Operational risk is inherent in all banking products, activities, processes and systems, and the effective management of operational risk has always been a fundamental element of a bank's risk management program. It seeks to identify why a loss happened and at the broadest level includes the breakdown by four causes: people, processes, systems and external factors. As a result, sound operational risk management is a reflection of the effectiveness of the board and senior management in administering its portfolio of products, activities, processes, and systems.

Risk management generally encompasses the process of identifying risks to the bank, measuring exposures to those risks (where possible), ensuring that an effective capital planning and monitoring programme is in place, monitoring risk exposures and corresponding capital needs on an ongoing basis, taking steps to control or mitigate risk exposures and reporting to senior management and the board on the bank's risk exposures and capital positions. Internal controls are typically embedded in a bank's day-to-day business and are designed to ensure, to the extent possible, that bank activities are efficient and effective, information is reliable, timely and complete, and the bank is compliant with applicable laws and regulation. In practice, the two notions are in fact closely related and the distinction between both is less important than achieving the objectives of each.

Sound internal governance forms the foundation of an effective operational risk management framework. Although internal governance issues related to the management of operational risk are not unlike those encountered in the management of credit or market risk, operational risk management challenges may differ from those in other risk areas. Common banking practice for sound operational risk governance often relies on three lines of defense:

1st Line of Defense - **Business Line Management**

The business line management is responsible for identifying and managing the risks inherent in the products, activities, processes and systems for which it is accountable.

2nd Line of Defense - **An Independent Corporate Operational Risk Management Function (CORF)**

The CORF generally complements the business line's operational risk management activities. The CORF has a reporting structure independent of the risk generating business lines and is responsible for the design, maintenance and ongoing development of the operational risk framework within the bank. This function may include the operational risk measurement and reporting processes, risk committees and responsibility for board reporting. A key function of the CORF is to challenge the business lines' inputs to, and outputs from, the bank's risk management, risk measurement and reporting systems. The CORF should have a sufficient number of personnel skilled in the management of operational risk to effectively address its many responsibilities.

3rd Line of Defense - **An Independent Review**

This line of defense challenges the bank's operational risk management controls, processes and systems. This review may be done by internal audit or by staff independent of the process or system under review, but may also involve suitably qualified external parties.

Internal audit coverage should be adequate to independently verify that the Framework has been implemented as intended and is functioning effectively. It should include opining on the overall appropriateness and adequacy of the framework and the associated governance processes across the bank. Internal audit should not simply be testing for compliance with board approved policies and procedures, but should also be evaluating whether the framework meets organizational needs and supervisory expectations.

Depending on the bank's nature, size and complexity, and the risk profile of a bank's activities, the degree of formality of how these three lines of defense are implemented will vary. A strong risk culture and good communication among the three lines of defense are important characteristics of good operational risk governance. In all cases, however, a bank's operational risk governance function should be fully integrated into the bank's overall risk management governance structure.

The Central Bank of Belize (Central Bank) has adopted ten principles to promote sound practices for managing operational risk. These Guidelines are founded on the Basel Committee of Banking Supervisors' *Principles for the Sound Management of Operational Risk*, June 2011.

The principles outlined in this Guideline will be used by the Central Bank to evaluate the operational risk management systems of banks licensed under the Domestic Banks and Financial Institutions Act (DBFIA) and the International Banking Act (IBA). Banks are expected to adopt operational risk management approaches commensurate with the scope and sophistication of their activities. These guidelines should be applied in concurrence with the requirements of the DBFIA, IBA, practice directions, and circulars issued by the Central Bank, and where applicable.

The Central Bank, as part of its ongoing supervisory responsibilities, intends to assess the degree of licensees' compliance with the principles set forth in these Guidelines, considering the nature, size, risk profile and complexity of the licensee's activities. Consequently, the Central Bank will examine the effectiveness of the operational risk management strategy and framework during its on-site examination of licensees.

PRINCIPLES OF OPERATIONAL RISK MANAGEMENT

FUNDAMENTAL PRINCIPLES OF OPERATIONAL RISK MANAGEMENT

Principle 1: *The Board of directors (Board) should take the lead in establishing a strong risk management culture. The Board and senior management should establish a corporate culture that is guided by strong risk management and that supports and provides appropriate standards and incentives for professional and responsible behaviour. In this regard, it is the responsibility of the Board to ensure that a strong operational risk management culture exists throughout the entire organization.*

Principle 2: *Banks should develop, implement and maintain a Framework that is fully integrated into the bank's overall risk management processes. The Framework for operational risk management chosen by an individual bank will depend on a range of factors, including its nature, size, complexity and risk profile.*

GOVERNANCE

THE BOARD OF DIRECTORS

Principle 3: *The Board should establish, approve and periodically review the Framework. The Board should oversee senior management to ensure that the policies, processes and systems are implemented effectively at all decision levels.*

Principle 4: *The Board should approve and review a risk appetite and tolerance statement[12] for operational risk that articulates the nature, types, and levels of operational risk that the bank is willing to assume.*

SENIOR MANAGEMENT

Principle 5: *Senior management should develop for approval by the Board a clear, effective and robust governance structure with well defined, transparent and consistent lines of responsibility. Senior management is responsible for consistently implementing and maintaining throughout the organization policies, processes and systems for managing operational risk in all of the bank's material products, activities, processes and systems consistent with its risk appetite and tolerance*.

RISK MANAGEMENT ENVIRONMENT

IDENTIFICATION AND ASSESSMENT

Principle 6: *Senior management should ensure the identification and assessment of the operational risk inherent in all material products, activities, processes and systems to make sure the inherent risks and incentives are well understood.*

Principle 7: *Senior management should ensure that there is an approval process for all new products, activities, processes and systems that fully assesses operational risk.*

MONITORING AND REPORTING

Principle 8: *Senior management should implement a process to regularly monitor operational risk profiles and material exposures to losses. Appropriate reporting mechanisms should be in place at the Board, senior management, and business line levels that support proactive management of operational risk.*

CONTROL AND MITIGATION

Principle 9: *Banks should have a strong control environment that utilizes policies, processes and systems; appropriate internal controls; and appropriate risk mitigation and/or transfer strategies.*

BUSINESS RESILIENCY AND CONTINUITY

Principle 10: *Banks should have business resiliency and continuity plans in place to ensure an ability to operate on an ongoing basis and limit losses in the event of severe business disruption*.

FUNDAMENTAL PRINCIPLES OF OPERATIONAL RISK MANAGEMENT

PRINCIPLE 1

The Board should take the lead in establishing a strong risk management culture. The Board and senior management should establish a corporate culture that is guided by strong risk management and that supports and provides appropriate standards and incentives for professional and responsible behaviour. In this regard, it is the responsibility of the Board to ensure that a strong operational risk management culture exists throughout the whole organization.

1.1 Banks with a strong culture of risk management and ethical business practices are less likely to experience potentially damaging operational risk events and are better placed to deal effectively with those events that do occur. The actions of the board and senior management, and policies, processes and systems provide the foundation for a sound risk management culture.

1.2 The Board should establish a code of conduct or an ethics policy that sets clear expectations for integrity and ethical values of the highest standard and identify acceptable business practices and prohibited conflicts. Clear expectations and accountabilities ensure that bank staff understand their roles and responsibilities for risk, as well as their authority to act. Strong and consistent senior management support for risk management and ethical behaviour convincingly reinforces codes of conduct and ethics, compensation strategies, and training programs. Compensation policies should be aligned to the bank's statement of risk appetite and tolerance, long-term strategic direction, financial goals and overall safety and soundness. They should also appropriately balance risk and reward.

1.3 Senior management should ensure that an appropriate level of operational risk training is available at all levels throughout the organization. Training that is provided should reflect the seniority, role and responsibilities of the individuals for whom it is intended.

PRINCIPLE 2

Banks should develop, implement and maintain a Framework that is fully integrated into the bank's overall risk management processes. The Framework for operational risk management chosen by an individual bank will depend on a range of factors, including its nature, size, complexity and risk profile.

2.1 The fundamental premise of sound risk management is that the Board and senior management understand the nature and complexity of the risks inherent in the portfolio of the bank's products, services and activities. This is particularly important for operational risk, given that operational risk is inherent in all business products, activities, processes and systems.

2.2 A vital means of understanding the nature and complexity of operational risk is to have the components of the Framework fully integrated into the overall risk management processes of the bank. The Framework should be appropriately integrated into the risk management processes across all levels of the organization including those at the group and business line levels, as well as into new business initiatives' products, activities, processes and systems. In addition, results of the bank's operational risk assessment should be incorporated into the overall bank business strategy development processes.

2.3 The Framework should be comprehensively and appropriately documented in Board-approved policies and should include definitions of operational risk and operational loss. Banks that do not adequately describe and classify operational risk and loss exposure may significantly reduce the effectiveness of their Framework.

2.4 Framework documentation should clearly:

a) identify the governance structures used to manage operational risk, including reporting lines and accountabilities;

b) describe the risk assessment tools and how they are used;

c) describe the bank's accepted operational risk appetite and tolerance, as well as thresholds or limits for inherent and residual risk, and approved risk mitigation strategies and instruments;

d) describe the bank's approach to establishing and monitoring thresholds or limits for inherent and residual risk exposure;

e) establish risk reporting and Management Information Systems (MIS);

f) provide for a common taxonomy of operational risk terms to ensure consistency of risk identification, exposure rating and risk management objectives;

g) provide for appropriate independent review and assessment of operational risk; and

h) require the policies to be reviewed whenever a material change in the operational risk profile of the bank occurs, and revised as appropriate.

GOVERNANCE

THE BOARD OF DIRECTORS

PRINCIPLE 3

The Board should establish, approve and periodically review the Framework. The Board should oversee senior management to ensure that the policies, processes and systems are implemented effectively at all decision levels.

3.1 The Board should:

a) establish a management culture, and supporting processes, to understand the nature and scope of the operational risk inherent in the bank's strategies and activities, and develop comprehensive, dynamic oversight and control environments that are fully integrated into or coordinated with the overall framework for managing all risks across the enterprise;

b) provide senior management with clear guidance and direction regarding the principles underlying the Framework and approve the corresponding policies developed by senior management;

c) regularly review the Framework (at least annually), to ensure that the bank has identified and is managing the operational risk arising from external market changes and other environmental factors, as well as those operational risks associated with new products, activities, processes or systems, including changes in risk profiles and priorities (eg changing business volumes);

d) ensure that the bank's Framework is subject to effective independent review by audit or other appropriately trained parties; and

e) ensure that as best practice evolves management is availing themselves of these advances.

3.2 Strong internal controls are a critical aspect of operational risk management, and the Board should establish clear lines of management responsibility and accountability for implementing a strong control environment. The control environment should provide appropriate independence/separation of duties between operational risk management functions, business lines and support functions.

PRINCIPLE 4

The Board should approve and review a risk appetite and tolerance statement for operational risk that articulates the nature, types and levels of operational risk that the bank is willing to assume.

4.1 When approving and reviewing the risk appetite and tolerance statement, the Board should consider all relevant risks, the bank's level of risk aversion, its current financial condition and the bank's strategic direction. The risk appetite and tolerance statement should encapsulate the various operational risk appetites within a bank and ensure that they are consistent. The Board should approve appropriate thresholds or limits for specific operational risks, and an overall operational risk appetite and tolerance.

4.2 The Board should regularly review the appropriateness of limits and the overall operational risk appetite and tolerance statement. This review should consider changes in the external environment, material increases in business or activity volumes, the quality of the control environment, the effectiveness of risk management or mitigation strategies, loss experience, and the frequency, volume or nature of limit breaches. The board should monitor management adherence to the risk appetite and tolerance statement and provide for timely detection and remediation of breaches.

SENIOR MANAGEMENT

PRINCIPLE 5

Senior management should develop for approval by the Board a clear, effective and robust governance structure with well defined, transparent and consistent lines of responsibility. Senior management is responsible for consistently implementing and maintaining the policies, processes and systems for managing operational risk in all of the bank's material products, activities, processes and systems consistent with the risk appetite and tolerance.

5.1 Senior management is responsible for establishing and maintaining robust challenge mechanisms and effective issue-resolution processes. These should include systems to report, track and, when necessary, escalate issues to ensure resolution. Banks should be able to demonstrate that the three lines of defense approach is operating satisfactorily and to explain how the board and senior management ensure that this approach is implemented and operating in an appropriate and acceptable manner.

5.2 Senior management should translate the operational risk management Framework established by the Board into specific policies and procedures that can be implemented and verified within the different business units. Senior management should clearly assign authority, responsibility and reporting relationships to encourage and maintain accountability, and to ensure that the necessary resources are available to manage operational risk in line within the bank's risk appetite and

tolerance statement. Moreover, senior management should ensure that the management oversight process is appropriate for the risks inherent in a business unit's activity.

5.3 Senior management should ensure that staff responsible for managing operational risk coordinate and communicate effectively with staff responsible for managing credit, market, and other risks, as well as with those in the bank who are responsible for the procurement of external services such as outsourcing arrangements. Failure to do so could result in significant gaps or overlaps in a bank's overall risk management programme.

5.4 The managers of the CORF should be of sufficient stature within the bank to perform their duties effectively, ideally evidenced by title commensurate with other risk management functions such as credit, market and liquidity risk.

5.5 Senior management should ensure that bank activities are conducted by staff with the necessary experience, technical capabilities and access to resources. Staff responsible for monitoring and enforcing compliance with the institution's risk policy should have authority independent from the units they oversee.

5.6 A bank's governance structure should be commensurate with the nature, size, complexity, and risk profile of its activities. When designing the operational risk governance structure, a bank should take the following into consideration:

a) *Committee structure* – Sound industry practice for larger and more complex organizations with a central group function and separate business units is to utilize a board-created enterprise level risk committee for overseeing all risks, to which a management level operational risk committee reports. Depending on the nature, size and complexity of the bank, the enterprise level risk committee may receive input from operational risk committees by business or functional area. Smaller and less complex organizations may utilize a flatter organizational structure that oversees operational risk directly within the board's risk management committee;

b) *Committee composition* – Sound industry practice is for operational risk committees (or the risk committee in smaller banks) to include a combination of members with expertise in business activities and financial, as well as independent risk management. Committee membership can also include independent non-executive board members; and

c) *Committee operation* – Committee meetings should be held at appropriate frequencies with adequate time and resources to permit productive discussion and decision-making. Records of committee operations should be adequate to permit review and evaluation of committee effectiveness.

RISK MANAGEMENT ENVIRONMENT

IDENTIFICATION AND ASSESSMENT

PRINCIPLE 6

Senior management should ensure the identification and assessment of the operational risk inherent in all material products, activities, processes and systems to make sure the inherent risks and incentives are well understood.

6.1 Risk identification and assessment are fundamental characteristics of an effective operational risk management system. Effective risk identification considers both internal factors[2] and external

factors.[3] Sound risk assessment allows the bank to better understand its risk profile and allocate risk management resources and strategies most effectively.

6.2 Examples of tools that may be used for identifying and assessing operational risk include:

a) *Internal/External Audit Findings* - While audit findings primarily focus on control weaknesses and vulnerabilities, they can also provide insight into inherent risk due to internal or external factors;

b) *Internal Loss Data Collection and Analysis* - Internal operational loss data provides meaningful information for assessing a bank's exposure to operational risk and the effectiveness of internal controls (see ANNEX I). Analysis of loss events can provide insight into the causes of losses and information on whether control failures are isolated or systematic. Banks may also find it useful to capture and monitor operational risk contributions to credit and market risk related losses in order to obtain a more complete view of their operational risk exposure;

c) *External Data Collection and Analysis* - External data elements consist of gross operational loss amounts, dates, recoveries, and relevant causal information for operational loss events occurring at organizations other than the bank. External loss data can be compared with internal loss data, or used to explore possible weaknesses in the control environment or consider previously unidentified risk exposures;

d) *Risk Assessments* - In a risk assessment, often referred to as a Risk Self-Assessment (RSA), a bank assesses the processes underlying its operations against a library of potential threats and vulnerabilities and considers their potential impact. A similar approach, Risk Control Self Assessments (RCSA), typically evaluates inherent risk (the risk before controls are considered), the effectiveness of the control environment, and residual risk (the risk exposure after controls are considered). Scorecards build on RCSAs by weighting residual risks to provide a means of translating the RCSA output into metrics that give a relative ranking of the control environment;

e) *Business Process Mapping* - Business process mappings identify the key steps in business processes, activities and organizational functions. They also identify the key risk points in the overall business process. Process maps can reveal individual risks, risk interdependencies, and areas of control or risk management weakness. They also can help prioritize subsequent management action;

f) *Risk and Performance Indicators* - Risk and performance indicators are risk metrics and/or statistics that provide insight into a bank's risk exposure. Risk indicators, often referred to as Key Risk Indicators (KRIs), are used to monitor the main drivers of exposure associated with key risks. Performance indicators, often referred to as Key Performance Indicators (KPIs), provide insight into the status of operational processes, which may in turn provide insight into operational weaknesses, failures, and potential loss. Risk and performance indicators are often paired with escalation triggers to warn when risk levels approach or exceed thresholds or limits and prompt mitigation plans;

g) *Scenario Analysis* - Scenario analysis is a process of obtaining expert opinion of business line and risk managers to identify potential operational risk events and assess their potential outcome. Scenario analysis is an effective tool to consider potential sources of significant operational risk and the need for additional risk management controls or mitigation solutions. Given the subjectivity of the scenario process, a robust governance framework is essential to ensure the integrity and consistency of the process;

h) *Measurement* - Larger banks may find it useful to quantify their exposure to operational risk by using the output of the risk assessment tools as inputs into a model that estimates operational risk exposure. The results of the model can be used in an economic capital process and can be allocated to business lines to link risk and return; and

i) *Comparative Analysis* - Comparative analysis consists of comparing the results of the various assessment tools to provide a more comprehensive view of the bank's operational risk profile. For example, comparison of the frequency and severity of internal data with RCSAs can help the bank determine whether self-assessment processes are functioning effectively. Scenario data can be compared to internal and external data to gain a better understanding of the severity of the bank's exposure to potential risk events.

6.3 The bank should ensure that the internal pricing and performance measurement mechanisms appropriately take into account operational risk. Where operational risk is not considered, risk-taking incentives might not be appropriately aligned with the risk appetite and tolerance.

6.4 As the risk profile and appetite of an institution may change over time, the assessment of operational risks should be conducted periodically along with the review of its tolerance levels. The frequency of periodic assessments and reviews is at the discretion of the licensee's Board and senior management. Nonetheless, periodic efforts are necessary as they ensure that material operational risks are captured through the continual update of a licensee's operational risk control strategies, policies, processes, procedures and systems.

PRINCIPLE 7

Senior management should ensure that there is an approval process for all new products, activities, processes and systems that fully assesses operational risk.

7.1 In general, a bank's operational risk exposure is increased when a bank engages in new activities or develops new products; enters unfamiliar markets; implements new business processes or technology systems; and/or engages in businesses that are geographically distant from the head office. Moreover, the level of risk may escalate when new products activities, processes, or systems transition from an introductory level to a level that represents material sources of revenue or business-critical operations. A bank should ensure that its risk management control infrastructure is appropriate at inception and that it keeps pace with the rate of growth of, or changes to, products activities, processes and systems.

7.2 A bank should have policies and procedures that address the process for review and approval of new products, activities, processes and systems. The review and approval process should consider:

a) inherent risks in the new product, service, or activity;

b) changes to the bank's operational risk profile and appetite and tolerance, including the risk of existing products or activities;

c) the necessary controls, risk management processes, and risk mitigation strategies;

d) the residual risk;

e) changes to relevant risk thresholds or limits; and

f) the procedures and metrics to measure, monitor, and manage the risk of the new product or activity.

7.3 The approval process should also ensure that appropriate investment has been made for human resources and technology infrastructure before new products are introduced. The implementation of new products, activities, processes and systems should be monitored in order to identify any material differences to the expected operational risk profile, and to manage any unexpected risks.

MONITORING AND REPORTING

PRINCIPLE 8

Senior management should implement a process to regularly monitor operational risk profiles and material exposures to losses. Appropriate reporting mechanisms should be in place at the board, senior management, and business line levels that support proactive management of operational risk.

8.1 Banks should continuously improve the quality of operational risk reporting. A bank should ensure that its reports are comprehensive, accurate, consistent and actionable across business lines and products. Reports should be manageable in scope and volume; effective decision-making is impeded by both excessive amounts and paucity of data.

8.2 Reporting should be timely and a bank should be able to produce reports in both normal and stressed market conditions. The frequency of reporting, at least on a quarterly basis, should reflect the risks involved and the pace and nature of changes in the operating environment. The results of monitoring activities should be included in regular management and board reports, as should assessments of the Framework performed by the internal audit and/or risk management functions. Reports generated by (and/or for) the Central Bank should also be reported internally to senior management and the board, where appropriate.

8.3 Operational risk reports may contain internal financial, operational, and compliance indicators, as well as external market or environmental information about events and conditions that are relevant to decision making. Operational risk reports should include:

a) breaches of the bank's risk appetite and tolerance statement, as well as thresholds or limits;

b) details of recent significant internal operational risk events and losses; and

c) relevant external events and any potential impact on the bank and operational risk capital.

8.4 Data capture and risk reporting processes should be analyzed periodically with a view to continuously enhancing risk management performance as well as advancing risk management policies, procedures and practices.

CONTROL AND MITIGATION

PRINCIPLE 9

Banks should have a strong control environment that utilizes policies, processes and systems; appropriate internal controls; and appropriate risk mitigation and/or transfer strategies.

9.1 On an ongoing basis, Banks should provide for expected losses and maintain adequate financial resources against unexpected losses that may be encountered in the normal course of their business activities.

Internal Controls

9.2 Internal controls should be designed to provide reasonable assurance that a bank will have efficient and effective operations, safeguard its assets, produce reliable financial reports, and comply with applicable laws and regulations. A sound internal control program consists of five components that are integral to the risk management process: control environment, risk assessment, control activities, information and communication, and monitoring activities.

9.3 Control processes and procedures should include a system for ensuring compliance with policies. Examples of principle elements of a policy compliance assessment include:

a) top-level reviews of progress towards stated objectives;

b) verifying compliance with management controls;

c) review of the treatment and resolution of instances of non-compliance;

d) evaluation of the required approvals and authorizations to ensure accountability to an appropriate level of management; and

e) tracking reports for approved exceptions to thresholds or limits, management overrides and other deviations from policy.

9.4 An effective control environment also requires appropriate segregation of duties. Assignments that establish conflicting duties for individuals or a team without dual controls or other countermeasures may enable concealment of losses, errors or other inappropriate actions. Therefore, areas of potential conflicts of interest should be identified, minimized, and be subject to careful independent monitoring and review.

9.5 In addition to segregation of duties and dual control, banks should ensure that other traditional internal controls are in place as appropriate to address operational risk. Examples of these controls include:

a) clearly established authorities and/or processes for approval;

b) close monitoring of adherence to assigned risk thresholds or limits;

c) safeguards for access to, and use of, bank assets and records;

d) appropriate staffing level and training to maintain expertise;

e) ongoing processes to identify business lines or products where returns appear to be out of line with reasonable expectations;
f) regular verification and reconciliation of transactions and accounts; and

g) a vacation policy that provides for officers and employees being absent from their duties for a period of not less than two consecutive weeks.

Information Technology

9.6 Effective use and sound implementation of technology can contribute to the control environment. For example, automated processes are less prone to error than manual processes. However, automated processes introduce risks that must be addressed through sound technology governance and infrastructure risk management programmes.

9.7 The use of technology related products, activities, processes and delivery channels exposes a bank to strategic, operational, reputational, and cyber risks and the possibility of material financial loss. Consequently, a bank should have an integrated approach to identifying, measuring, monitoring and managing technology risks.21 Sound technology risk management uses the same precepts as operational risk management and includes:

a) governance and oversight controls that ensure technology, including outsourcing arrangements, is aligned with and supportive of the bank's business objectives;

b) policies and procedures that facilitate identification and assessment of risk;

c) establishment of a risk appetite and tolerance statement as well as performance expectations to assist in controlling and managing risk;

d) implementation of an effective control environment and the use of risk transfer strategies that mitigate risk; and

e) monitoring processes that test for compliance with policy thresholds or limits.

9.8 Management should ensure the bank has a sound technology infrastructure that meets current and long-term business requirements by providing sufficient capacity for normal activity levels as well as peaks during periods of market stress; ensuring data and system integrity, security, and availability; and supporting integrated. and comprehensive risk management. Banks should also ensure that its information technology infrastructure at minimum meet the benchmarks established by the Central Bank in the Cyber Security Guidelines issued in xx 2019.

Outsourcing and Insurance

9.9 Outsourcing is the use of a third party – either an affiliate within a corporate group or an unaffiliated external entity – to perform activities on behalf of the bank. Outsourcing can involve transaction processing or business processes. While outsourcing can help manage costs, provide expertise, expand product offerings, and improve services, it also introduces risks that management should address. The board and senior management are responsible for understanding the operational risks associated with outsourcing arrangements and ensuring that effective risk management policies and practices are in place to manage the risk in outsourcing activities. Outsourcing policies and risk management activities should encompass:

a) procedures for determining whether and how activities can be outsourced;

b) processes for conducting due diligence in the selection of potential service providers;

c) sound structuring of the outsourcing arrangement, including ownership and confidentiality of data, as well as termination rights;

d) programs for managing and monitoring the risks associated with the outsourcing arrangement, including the financial condition of the service provider;

e) establishment of an effective control environment at the bank and the service provider;

f) development of viable contingency plans; and

g) execution of comprehensive contracts and/or service level agreements with a clear allocation of responsibilities between the outsourcing provider and the bank.

9.10 In those circumstances where internal controls do not adequately address risk and exiting the risk is not a reasonable option, management can complement controls by seeking to transfer the risk to another party such as through insurance. The Board should determine the maximum loss exposure the bank is willing and has the financial capacity to assume, and should perform an annual review of the bank's risk and insurance management program.

9.11 Because risk transfer is an imperfect substitute for sound controls and risk management programs, banks should view risk transfer tools as complementary to, rather than a replacement for, thorough internal operational risk control. Having mechanisms in place to quickly identify, recognize and rectify distinct operational risk errors can greatly reduce exposures. Careful consideration also needs to be given to the extent to which risk mitigation tools such as insurance truly reduce risk, transfer the risk to another business sector or area, or create a new risk (e.g. counterparty risk).

BUSINESS RESILIENCY AND CONTINUITY

PRINCIPLE 10

Banks should have business resiliency and continuity plans in place to ensure an ability to operate on an ongoing basis and limit losses in the event of severe business disruption.

10.1 Banks are exposed to disruptive events, some of which may be severe and result in an inability to fulfil some or all of their business obligations. Incidents that damage or render inaccessible the bank's facilities, telecommunication or information technology infrastructures, or a pandemic event that affects human resources, can result in significant financial losses to the bank, as well as broader disruptions to the financial system. To provide resiliency against this risk, a bank should establish business continuity plans commensurate with the nature, size and complexity of their operations. Such plans should take into account different types of likely or plausible scenarios to which the bank may be vulnerable.

10.2 Continuity management should incorporate business impact analysis, recovery strategies, testing, training and awareness programs, and communication and crisis management programs. A bank should identify critical business operations,[4] key internal and external dependencies,[5] and appropriate resilience levels. Plausible disruptive scenarios should be assessed for their financial, operational, liquidity and reputational impact, and the resulting risk assessment should be the foundation for recovery priorities and objectives. Continuity plans should establish contingency strategies, recovery and resumption procedures, and communication plans for informing management, employees, regulatory authorities, customer, suppliers, and – where appropriate – civil authorities.

10.3 A bank should periodically review its continuity plans to ensure contingency strategies remain consistent with current operations, risks and threats, resiliency requirements, and recovery priorities. Training and awareness programs should be implemented to ensure that staff can effectively execute contingency plans. Plans should be tested periodically to ensure that recovery and resumption objectives and timeframes can be met. Where possible, a bank should participate in disaster recovery and business continuity testing with key service providers. Results of formal testing activity should be reported to management and the board.

ANNEX I

Internal Loss Data Collection and Analysis

The proper identification, collection and treatment of internal loss data are essential prerequisites to operational risk management. A bank's internal loss data must be comprehensive and capture all material activities and exposures from all appropriate subsystems and geographic locations.

Internal loss data needs to be clearly linked to the bank's current business activities, technological processes and risk management procedures. Therefore, a bank must have documented procedures and processes for the identification, collection and treatment of internal loss data. Such procedures and processes must be subject to validation and to regular independent reviews by internal and/or external audit functions.

For risk management purposes, and to assist in supervisory validation and/or review, the historical internal loss data collected by banks is to be mapped into the relevant supervisory event categories as defined by the Basel Framework and should be available whenever the supervisor requires it. The bank must document criteria for allocating losses to the specified event types.

Banks must have processes to independently review the comprehensiveness and accuracy of loss data.

Building an acceptable loss data set from the available internal data requires that the bank develop policies and procedures to address several features, including gross loss definition, reference date and grouped losses.

Gross loss is a loss before recoveries of any type. Net loss is defined as the loss after taking into account the impact of recoveries. The recovery is an independent occurrence, related to the original loss event, separate in time, in which funds or inflows of economic benefits are received from a third party. Examples of recoveries are payments received from insurers, repayments received from perpetrators of fraud, and recoveries of misdirected transfers.

Banks must be able to identify the gross loss amounts, non-insurance recoveries, and insurance recoveries for all operational loss events. Banks should use losses net of recoveries (including insurance recoveries) in the loss dataset. However, recoveries can be used to reduce losses only after the bank receives payment. Receivables do not count as recoveries. Verification of payments received to net losses must be provided to supervisors upon request.

The following items must be included in the gross loss:

a) Direct charges, including impairments and settlements, to the bank's P&L accounts and write-downs due to the operational risk event;
b) Costs incurred as a consequence of the event including external expenses with a direct link to the operational risk event (eg legal expenses directly related to the event and fees paid to advisors, attorneys or suppliers) and costs of repair or replacement, incurred to restore the position that was prevailing before the operational risk event;
c) Provisions or reserves accounted for in the P&L against the potential operational loss impact;
d) Losses stemming from operational risk events with a definitive financial impact, which are temporarily booked in transitory and/or suspense accounts and are not yet reflected in the P&L ("pending losses"). Material pending losses should be included in the loss data set within a time period commensurate with the size and age of the pending item; and
e) Negative economic impacts booked in a financial accounting period, due to operational risk events impacting the cash flows or financial statements of previous financial accounting periods (timing losses"). Material "timing losses" should be included in the loss

data set when they are due to operational risk events that span more than one financial accounting period and give rise to legal risk.

The following items should be excluded from the gross loss computation:

a) Costs of general maintenance contracts on property, plant or equipment;
b) Internal or external expenditures to enhance the business after the operational risk losses: upgrades, improvements, risk assessment initiatives and enhancements; and
c) Insurance premiums.

Banks must use the date of accounting for building the loss data set. The bank must use a date no later than the date of accounting for including losses related to legal events in the loss data set. For legal loss events, the date of accounting is the date when a legal reserve is established for the probable estimated loss in the P&L.

Losses caused by a common operational risk event or by related operational risk events over time, but posted to the accounts over several years, should be allocated to the corresponding years of the loss database, in line with their accounting treatment.

Required data fields to be reported for each operational risk event:

a) *Identity number* - Each loss event needs to be identified in a sequential and univocal manner.

b) *Event nature* - One of the following labels needs to be selected:
   i. Individual loss
   ii. Repetitive loss
   iii. Accounting provision
   iv. Reversal or adjustment of an accounting provision
   v. Recovery

c) *Link* - Whenever several events are linked, this field should allow to link the reported event with its root event whenever possible (for example for recoveries, or adjustments of provisions.).

d) Dates to be reported
   i. Date of occurrence (if known)
   ii. Date of discovery
   iii. Date of accounting (when a loss event results in a loss, reserve or provision against a loss being recognised in the bank's profit and loss accounts)
   iv. Date of closure of the event (if known).

   Events should always be reported as soon as possible after discovered.

e) *Description* - A short description of the event should be included indicating what caused the event in the first place. The degree of detail should be proportional its severity.

f) *Type of event* - Each event needs to be mapped into the relevant supervisory categories (see ANNEX II). The bank must document criteria for allocating losses to the specified event types. The main criteria to decide on the type of event should be given by the answer: What happened for the event to occur?

g) *Product / Service* - Most event types come linked to a product or service. It may be left as a text string for the bank to decide or use the categories of ORRS[1].

h) *Process* - Most event types occur within a process. It may be left as a text string for the bank to decide or use the categories of ORRS[2].

i) *Gross loss;* and

j) *Balance sheet account impacted*.

[1] ORX: "*Operational Risk Reporting Standards (ORRS)*", Ed.2017 v.1.4, rev. March 2018.
[2] Ibid

ANNEX II

Table I: Detailed Loss Event Type Classification

Event-Type Category (Level 1)	Definition	Categories (Level 2)	Activity Examples (Level 3)
Internal fraud	Losses due to acts of a type intended to defraud, misappropriate property or circumvent regulations, the law or company policy, excluding diversity/ discrimination events, which involves at least one internal party	Unauthorised Activity	• Transactions not reported (intentional) • Transaction type unauthorised (w/monetary loss) • Mismarking of position (intentional)
		Theft and Fraud	• Fraud / credit fraud / worthless deposits • Theft / extortion / embezzlement / robbery • Misappropriation of assets • Malicious destruction of assets • Forgery • Check kiting • Smuggling • Account take-over / impersonation / etc. • Tax non-compliance / evasion (wilful) • Bribes / kickbacks • Insider trading (not on firm's account)
External Fraud	Losses due to acts of a type intended to defraud, misappropriate property or circumvent the law, by a third party	Theft and Fraud	• Theft/Robbery • Forgery • Check kiting
		Systems Security	• Hacking damage • Theft of information (w/monetary loss)
Employment Practices and Workplace Safety	Losses arising from acts inconsistent with employment, health or safety laws or agreements, from payment of personal injury claims, or from diversity / discrimination events	Employee Relations	• Compensation, benefit, termination issues • Organised labour activity
		Safe Environment	• General liability (slip and fall, etc.) • Employee health & safety rules events • Workers compensation
		Diversity & Discrimination	• All discrimination types
Clients, Products and Business Practices	Losses arising from an unintentional or negligent failure to meet a professional obligation to specific clients (including fiduciary and suitability	Suitability, Disclosure & Fiduciary	• Fiduciary breaches / guideline violations • Suitability / disclosure issues (KYC, etc.) • Retail customer disclosure violations • Breach of privacy • Aggressive sales • Account churning • Misuse of confidential information • Lender liability

	requirements), or from the nature or design of a product.	Improper Business or Market Practices	• Antitrust • Improper trade / market practices • Market manipulation • Insider trading (on firm's account) • Unlicensed activity • Money laundering
		Product Flaws	• Product defects (unauthorised, etc.) • Model errors
		Selection, Sponsorship & Exposure	• Failure to investigate client per guidelines • Exceeding client exposure limits
		Advisory Activities	• Disputes over performance of advisory activities
Damage to Physical Assets	Losses arising from loss or damage to physical assets from natural disaster or other events	Disasters and other events	• Natural disaster losses • Human losses from external sources (terrorism, • vandalism)
Business disruption and system failures	Losses arising from disruption of business or system failures	Systems	• Hardware • Software • Telecommunications • Utility outage / disruptions
Execution, Delivery & Process Management	Losses from failed transaction processing or process management, from relations with trade counterparties and vendors	Transaction Capture, Execution & Maintenance	• Miscommunication • Data entry, maintenance or loading error • Missed deadline or responsibility • Model / system misoperation • Accounting error / entity attribution error • Other task misperformance • Delivery failure • Collateral management failure • Reference Data Maintenance
		Monitoring and Reporting	• Failed mandatory reporting obligation • Inaccurate external report (loss incurred)
		Customer Intake and Documentation	• Client permissions / disclaimers missing • Legal documents missing / incomplete
		Customer / Client Account Management	• Unapproved access given to accounts • Incorrect client records (loss incurred) • Negligent loss or damage of client assets
		Trade Counterparties	• Non-client counterparty malperformance • Misc. non-client counterparty disputes

		Vendors & Suppliers	• Outsourcing • Vendor disputes