ANNEX 1:

GUIDELINES ON OPERATIONAL RISK MANAGEMENT

FOR BANKS

Date: 14 July 2022

TABLE OF CONTENTS

1. INTRODUCTION

1.1. **Operational risk is defined as the risk of loss resulting from inadequate or failed internal processes, people and systems including internal frauds, or from external events including external frauds. This definition includes legal risks, but excludes strategic and reputational risk.** Legal risk is the risk arising from the potential that unenforceable contracts, lawsuits or adverse judgments may disrupt or otherwise negatively affect the operations or financial condition of a bank.

1.2. Operational risk is inherent in all banking products, activities, processes and systems. Sound operational risk governance, therefore, relies upon three lines of defence:

i) business unit management,
ii) an independent operational risk management unit (ORMU); and
iii) independent assurance.

2. GOVERNANCE

2.1. BOARD

2.1.1. **In general, the board should establish, approve and periodically review the operational risk management framework (ORMF). In addition, the board should oversee material operational risks and the effectiveness of key controls, and ensure that senior management implements the policies, processes and systems of the ORMF effectively at all decision levels.**

2.1.2. Specifically, the board should:

(a) Ensure the bank has adequate processes for understanding the nature and scope of the operational risk inherent in the bank's current and planned strategies and activities;

(b) Ensure that the operational risk management processes are subject to comprehensive and dynamic oversight that are fully integrated into or coordinated with the overall framework for managing all risks across the bank;

(c) Provide senior management with clear guidance regarding the principles underlying the ORMF and ensure that corresponding policies developed by senior management are aligned with these principles;

(d) Regularly challenge senior management on the design and effectiveness of the bank's ORMF and approve and review the ORMF to ensure 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 (e.g. changing business volumes);

(e) Ensure the bank's ORMF is subject to effective independent review by a third line of defence (audit or other appropriately trained independent third parties;

(f) Ensure that, the bank is availing itself to new advances as best practice evolves;

(g) Take the lead in establishing a strong operational risk management culture in the bank, implemented by senior management, that provides appropriate standards for effectively managing operational risk and provides incentives for promoting professional and responsible behavior.

RISK APPETITE AND TOLERANCE STATEMENT

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

2.1.4. The risk appetite and tolerance statement for operational risk should be developed under the authority of the board and linked to the bank's short- and long-term strategic and financial plans. Taking into account the interests of the bank's customers and shareholders as well as regulatory requirements, an effective risk appetite and tolerance statement should:

(a) Be easy to communicate and therefore easy for all stakeholders to understand;

(b) Include key background information and assumptions that informed the bank's business plans at the time it was approved;

(c) Include statements that clearly articulate the motivations for taking on or avoiding certain types of risk, and establish boundaries or indicators (which may be quantitative or not) to enable monitoring of these risks;

(d) Ensure the strategy and risk limits of each business unit and legal entity, as relevant, align with the bank-wide risk appetite statement;

(e) Be forward-looking and, where applicable, subject to scenario and stress testing to ensure that the bank understands what events might push it outside its risk appetite and tolerance statement.

2.1.5. The board should approve and regularly review the appropriateness of limits and the overall operational risk appetite and tolerance statement. This review should consider current and expected changes in the external environment (including the regulatory context across all jurisdictions where the institution provides services); ongoing or forthcoming 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.

2.1.6. Limits should be set by considering quantitative metrics as well as qualitative analysis of major operational risk exposures. Where limitations in operational risk measurement methodologies may hamper the use of quantitative measures, qualitative factors such as the assessment of the causal and impact of operational

risk events should be used to determine the appropriate limits to effectively manage and contain exposures to all major operational risks.

2.2. SENIOR MANAGEMENT

2.2.1. **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.**

2.2.2. **Senior management is responsible for consistently implementing and maintaining throughout the organisation's policies, processes and systems for managing operational risk in all of the bank's material products, activities, processes and systems consistent with the bank's risk appetite and tolerance statement.**

2.2.3. 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 defence approach is operating effectively and to explain how the board, independent audit committee and senior management ensure that this approach is implemented and operating in an appropriate manner.

2.2.4. Senior management should translate the ORMF approved 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 the necessary resources are available to manage operational risk in line with 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.

2.2.5. Senior management should ensure that the ORMF's policies, processes and systems remain sufficiently robust to manage and ensure that operational losses are adequately addressed in a timely manner.

2.2.6. 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 insurance risk transfer and other third party arrangements (including outsourcing). Failure to do could result in significant gaps or overlaps in a bank's overall risk management programme.

2.2.7. Senior management should ensure that bank activities are conducted by staff with the relevant experience, qualification 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.

2.2.8. 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;
(b) Committee composition; and
(c) Committee operation.

SUCCESSION PLANNING

2.2.9. Banks should document their board-approved succession plans for their senior management team. Succession planning is an essential precautionary measure for a bank if its leadership stability, and hence ultimately its financial stability, is to be protected. Succession planning is especially critical for smaller institutions, where management teams tend to be smaller and possibly reliant on a few key individuals.

2.3. OPERATIONAL RISK MANAGEMENT UNIT (ORMU)

2.3.1. **Banks should establish, commensurate with its nature, size and complexity, an enterprise-wide Operational Risk Management Unit (ORMU), independent of the risk generating business lines, which is responsible for the design, maintenance and ongoing development of the ORMF within the bank. The ORMU should be adequately staffed with skilled resources (please refer to paragraph 2.2.7).**

2.3.2. Banks should have a policy which defines clear roles and responsibilities of the ORMU.

2.3.3. The responsibilities of an ORMU which is effectively the second line of defence should include:

a) Developing an independent view regarding business units' (i) identified material operational risks, (ii) design and effectiveness of key controls and (iii) risk tolerance;

b) Challenging the relevance and consistency of business units' implementation of the operational risk management tools, measurement activities and reporting systems via a quality assurance programme, and providing evidence of this effective challenge;

c) Developing and maintaining operational risk management and measurement policies, standards and guidelines;

d) Reviewing and contributing to the monitoring and reporting of the operational risk profile;

e) Designing and providing operational risk training and awareness.

2.3.4. The degree of independence of the ORMU may differ among banks. In small banks, independence may be achieved through separation of duties and independent review of processes and functions. In larger banks, the ORMU should

have a reporting structure independent of the risk generating business units and be responsible for the design, maintenance and ongoing development of the ORMF within the bank. ORMU typically engages relevant business control groups (e.g. compliance, legal, finance, and IT) to support its assessment of the operational risks and controls.

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

3. OPERATIONAL RISK MANAGEMENT FRAMEWORK (ORMF)

3.1. OVERVIEW

3.1.1. **Banks should develop, implement and maintain an operational risk management framework (ORMF) that is effective and efficient in identifying, assessing, monitoring and controlling/mitigating operational risk.**

3.1.2. **ORMF should be fully integrated into the bank's overall risk management processes. The ORMF adopted by an individual bank will depend on a range of factors, including the bank's nature, size, complexity and risk profile.**

3.1.3. The board and senior management should understand the nature and complexity of the risks inherent in the portfolio of bank products, services, activities and systems, which is a fundamental premise of sound risk management. This is particularly important for operational risk, given operational risk is inherent in all business products, activities, processes and systems.

3.1.4. The components of the ORMF should be fully integrated into the overall risk management processes of the bank by the first line of defence, adequately reviewed and challenged by the second line of defence, and independently reviewed by the third line of defence. The ORMF should be embedded across all levels of the organization including group and business units as well as new business initiatives' products, activities, processes and systems. In addition, results of the bank's overall operational risk assessment should be incorporated into the overall bank business strategy development process.

3.1.5. The ORMF should be comprehensively and appropriately documented in the board's approved policies and should include definitions of operational risk and operational loss.

3.1.6. ORMF documentation should clearly:

(a) Identify the governance structures used to manage operational risk, including reporting lines and accountabilities, and the mandates and membership of the operational risk governance committees;

(b) Identify policy for approval of policies by the board;

(c) Describe the tools for risk and control identification and assessment and the role and responsibilities of the three lines of defence in using them;

(d) Describe the bank's accepted operational risk appetite and tolerance; the thresholds, activity triggers or limits for inherent and residual risk; and the approved risk mitigation strategies and instruments;

(e) Describe the bank's approach to ensure controls are designed, implemented and operating effectively;

(f) Describe the bank's approach to establishing and monitoring thresholds or limits for inherent and residual risk exposure;

(g) Describe risks and controls implemented by all business units (e.g. in a control library)

(h) Establish risk reporting and management information systems (MIS) producing timely, and accurate data;

(i) Provide for a common taxonomy of operational risk terms to ensure consistency of risk identification, exposure rating and risk management objectives across all business units.[1] The taxonomy can distinguish operational risk exposures by event types, causes, materiality and business units where they occur; it can also flag those operational exposures that partially or entirely represent legal (including conduct), model and ICT (including cyber) risks as well as exposures in the credit or market risk boundary;

(j) Provide for appropriate independent review and challenge of the outcomes of the operational risk management process; and

(k) Require the policies to be reviewed and revised as appropriate based on continued assessment of the quality of the control environment addressing internal and external environmental changes or whenever a material change in the operational risk profile of the bank occurs.

3.2. IDENTIFICATION AND ASSESSMENT

3.2.1. **Senior management should ensure the comprehensive 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.**

3.2.2. Risk identification and assessment are fundamental characteristics of an effective operational risk management system. Effective risk identification considers both internal factors and external factors. Sound risk assessment allows the bank to better understand its risk profile and allocate risk management resources and strategies most effectively. Banks may use the classification categories contained in **APPENDIX 1** for determining and classifying operational risk events.

[1] An inconsistent taxonomy of operational risk terms may increase the likelihood of failure to identify and categorise risks, or failure to allocate responsibility for the assessment, monitoring, control and mitigation of risks.

3.2.3. Examples of tools used for identifying and assessing operational risk include the following and as elaborated further in **APPENDIX 2**:

(a) Operational risk event data
(b) Self-assessments
(c) Event management
(d) Control monitoring and assurance framework
(e) Metrics
(f) Scenario Analysis
(g) Benchmarking and comparative analysis

3.2.4. Banks should ensure that the operational risk assessment tools' outputs are:

(a) Based on accurate data, whose integrity is ensured by strong governance and robust verification and validation procedures;

(b) Adequately taken into account in the internal pricing and performance measurement mechanisms as well as for business opportunities assessments;

(c) Subject to ORMU monitored action plans or remediation plans when necessary.

3.3. NEW PRODUCTS, ACTIVITIES, PROCESSES AND SYSTEMS

3.3.1. **Senior management should ensure that the bank's change management process is comprehensive, appropriately resourced and include continuous risk and control assessments, adequately articulated between the relevant lines of defence.**

3.3.2. A bank's operational risk exposure evolves when a bank initiates change, such as engaging in new activities or developing new products or services; entering into unfamiliar markets or jurisdictions; implementing new or modifying business processes or technology systems; and/or engaging in businesses that are geographically distant from the head office. Change management should assess the evolution of associated risks across time, from inception to termination (i.e. throughout the full life-cycle of a product).[2]

3.3.3. A bank should have policies and procedures defining the process for identifying, managing, challenging, approving and monitoring change on the basis of agreed objective criteria. Change implementation should be monitored by specific oversight controls. Change management policies and procedures should be subject to independent and regular review and update, and clearly allocate roles

[2] The life cycle of a product or service encompasses various stages from the development, on-going changes, grandfathering and closure. Indeed, the level of risk may escalate for example 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.

and responsibilities in accordance with the three-line-of-defence approach, in particular:

(a) The first line of defence should perform operational risk and control assessments of new products and initiatives.

(b) The second line of defence (ORMU) should challenge the operational risk and control assessments of first line of defence, as well as monitor the implementation of appropriate controls or remediation actions. ORMU should cover all phases of this process, from the identification and evaluation of the required change, through the decision-making and planning phases, to the implementation and post-implementation review. In addition, ORMU should ensure that all relevant control groups (e.g. finance, compliance, legal, business, ICT, risk management) are involved as appropriate.

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

(a) Inherent and residual risks – including legal, ICT and model risks – in the launch of new products, services, activities, operations in unfamiliar markets, and in the implementation of new processes, people and systems (especially when outsourced);

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

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

(d) Changes to relevant risk thresholds or limits; and

(e) The procedures and metrics to assess, monitor, and manage the risk of new products, services, activities, markets, jurisdictions, processes and systems.

3.3.5. The review and approval process should include ensuring that appropriate investment has been made for human resources and technology infrastructure before changes are introduced. Changes should be monitored, during and after their implementation, to identify any material differences to the expected operational risk profile and manage any unexpected risks.

3.3.6. Banks should maintain a central record of their products and services to the extent possible (including the outsourced ones) to facilitate the monitoring of changes.

3.4. MONITORING AND REPORTING

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

3.4.2. 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 units and products. To this end, the first line of defence should ensure reporting on any residual operational risks, including operational risk events, control deficiencies, process inadequacies, and non-compliance with operational risk tolerances. Reports should be manageable in scope and volume by providing an outlook on the bank's operational risk profile and adherence to the operational risk appetite and tolerance statement; effective decision-making is impeded by both excessive amounts and paucity of data.

3.4.3. Reporting should be timely and a bank should be able to produce reports in both normal and stressed market conditions. The frequency of reporting 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 ORMF performed by the internal/external audit and/or risk management functions. Reports generated by or for the BDCB should also be reported internally to senior management and the board, where appropriate.

3.4.4. Operational risk reports should describe the operational risk profile of the bank by providing 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, limits or qualitative requirements;
(b) Discussion of key and emerging risk assessed and monitored by metrics;
(c) Details of recent significant internal operational risk events and losses (including root cause analysis);
(d) Relevant external events or regulatory changes and any potential impact on the bank.

3.4.5. Data capture and risk reporting processes should be analyzed periodically with the goal of continuously enhancing risk management performance as well as advancing risk management policies, procedures and practices.

3.4.6. A bank should report any significant operational risk developments[3] to BDCB.

[3] For reporting on IT incidents, refer to BDCB's Notice on Early Detection of Cyber Intrusion and Incident Reporting, as may be revised from time to time.

For reporting on fraud incidents, refer to BDCB's Notice on Reporting of Fraud Incidents, as may be revised from time to time

3.5. CONTROL AND MITIGATION

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

3.5.2. Strong internal controls are a critical aspect of operational risk management. The board should establish clear lines of management responsibility and accountability for implementing a strong control environment. Controls should be regularly reviewed, monitored, and tested to ensure ongoing effectiveness. The control environment should provide appropriate independence/separation of duties between operational risk management functions, business units and support functions.

3.5.3. 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 programme consists of five components that are integral to the risk management process: management oversight and control culture, risk assessment, control activities, information and communication, and monitoring activities.[4]

3.5.4. Control processes and procedures should include a system for ensuring compliance with policies, regulations and laws. 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, regulations and laws.

3.5.5. 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 result in concealment of losses, errors or other inappropriate actions. Therefore, areas where conflicts of interest may arise should be identified, minimized, and be subject to careful independent monitoring and review.

3.5.6. In addition to segregation of duties and dual controls, 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;

[4] Refer to BDCB's Guidelines on Internal Control Systems, as may be revised from time to time

(d) Appropriate staffing levels and training to maintain technical expertise;
(e) Ongoing processes to identify business units or products where returns appear to be out of line with reasonable expectations;
(f) Regular verification and reconciliation of transactions and accounts; and
(g) Vacation policy that provides for officers and employees being absent from their duties for a period of not less than two consecutive weeks.

3.5.7. Control reviews and audits should include fraud risk as part of their assessments. A bank's risk management framework and system of internal controls should be designed to:
(a) prevent and detect fraud (including suspected or allegations of fraud) appropriately; and
(b) respond to fraud, suspected fraud, or allegations of fraud.

3.5.8. 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.

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

3.5.10. In those circumstances where internal controls do not adequately address (i.e. assess or measure) risk and exiting the risk is not a reasonable option, senior 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 programme. While the specific insurance or risk transfer needs of a bank should be determined on an individual basis, many jurisdictions have regulatory requirements that must be considered.

3.5.11. Because risk transfer is an imperfect substitute for sound controls and risk management programmes, 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 – or specific legal risk exposure - 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).

4. OUTSOURCING

4.1. **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.**[5] Amongst others, the concentration of risk and the complexity of outsourcing should be taken into account. Third party risk 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) programmes 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 (what should include a register of outsourced activities);
(f) development of viable contingency plans;
(g) execution of comprehensive contracts and/or service level agreements with a clear allocation of responsibilities between the outsourcing provider and the bank.

5. INFORMATION AND COMMUNICATION TECHNOLOGY

5.1. **Banks should implement robust Information and Communication Technology[6] (ICT) governance that is consistent with their risk appetite and tolerance statement for operational risk and ensures that their ICT fully supports and facilitates their operations.**

5.2. **ICT should be subject to appropriate risk identification, protection, detection, response and recovery programmes that are regularly tested, incorporate appropriate situational awareness, and convey relevant information to users on a timely basis.**

5.3. The appropriate use and implementation of a sound ICT framework contribute to the effectiveness of the control environment and are fundamental to the achievement of a bank's strategic objectives. The ICT framework should reduce a bank's risk exposure to direct losses, legal claims, reputational damage, ICT disruption and misuse of technology in alignment with its risk appetite and tolerance statement.

[5] Refer to BDCB's Guidelines on Outsourcing, as may be revised from time to time
[6] Refer to BDCB's Guidelines on Information Technology Risk Management and Notice on Early Detection of Cyber Intrusion and Incident Reporting, as may be revised from time to time

6. BUSINESS CONTINUITY PLANNING

6.1. **Banks should have business continuity plans[7] in place to ensure their ability to operate on an ongoing basis and limit losses in the event of a severe business disruption.**

6.2. Sound and effective governance of banks' business continuity policy requires:

(a) The validation and regular review by the board;
(b) The strong involvement of the senior management and business units leaders in its implementation;
(c) The commitment of first and second lines of defence to its design;
(d) Regular review by the third line of defence.

6.3. Banks should prepare forward-looking business continuity plans (BCP) with scenario analyses associated with relevant impact assessments and recovery procedures.

(a) A bank should ground its business continuity policy on scenario analyses of potential disruptions that identify and categorize critical business operations and key internal or
(b) external dependencies. In doing so, banks should cover all their business units as well as critical providers and major third parties (e.g. central banks, clearing house).

(c) Each scenario should be subject to a quantitative and qualitative impact assessment or business impact analysis (BIA) with regards to its financial, operational, legal and reputational consequences.

(d) Each disruption scenario should be subject to thresholds or limits (such as maximum tolerable outage) for the activation of a business continuity procedure. The procedure should address resumption aspects, set recovery time objectives (RTO) and recovery point objectives (RPO) as well as communication guidelines for informing management, employees, regulatory authorities, customer, suppliers, and – where appropriate – civil authorities.

6.4. A bank should periodically review all components of its business continuity policy to ensure that contingency strategies remain consistent with current operations, risks and threats.

6.5. Business continuity procedures should be tested periodically to ensure that recovery and resumption objectives and timeframes can be met. Where possible, a bank should participate in business continuity testing with key service providers. Results of formal testing and review activities should be reported to senior management and the board.

6.6. Training and awareness programmes should be customized based on specific roles to ensure that staff can effectively execute contingency plans.

[7] Refer to BDCB's Guidelines on Risk Management Framework (paragraph 105 of Annex 1), as may be revised from time to time

7. ROLE OF DISCLOSURE[8]

7.1. **Banks should have a formal disclosure policy that is subject to regular and independent review and approval by the board.** The policy should address the bank's approach for determining what operational risk disclosures it will make and the internal controls over the disclosure process. In addition, banks should implement a process for assessing the appropriateness of their disclosures and disclosure policy.

7.2. A bank's public disclosure of relevant operational risk management information can lead to transparency and the development of better industry practice through market discipline. The amount and type of disclosure should be commensurate with the size, risk profile and complexity of a bank's operations, and evolving industry practice.

7.3. A bank should disclose its ORMF in a manner that allows stakeholders to determine whether the bank identifies, assesses, monitors and controls/mitigates operational risk effectively.

7.4. Banks should disclose relevant operational risk exposure information to their stakeholders (including significant operational loss events), while not creating operational risk through this disclosure (e.g. description of unaddressed control vulnerabilities).

[8] Refer to BDCB's Notice on Pillar 3 - Public Disclosure Requirements, as may be revised from time to time

GLOSSARY

The following terms, unless the context require otherwise, have the following meanings:

Term		Meaning
"board"	:	board of directors (for banks incorporated in Brunei Darussalam) or by its group/regional office or equivalent oversight function for the operations in Brunei Darussalam (for banks registered in Brunei Darussalam)
"group"	:	includes the bank's Head Office or parent company, subsidiaries[9], affiliates[10], and any entity (including their subsidiaries, affiliates and special purpose entities[11]) that the bank exerts control over or that exerts control over the bank.
"Information and Communication Technology"	:	the underlying physical and logical design of information technology and communication systems, the individual hardware and software components, data, and the operating environments.
"risk appetite"	:	The aggregate level and types of risk a bank is willing to assume, decided in advance and within its risk capacity, to achieve its strategic objectives and business plan.
"risk tolerance"	:	The variation around the prescribed risk appetite that the bank is willing to tolerate.
"senior management"	:	The CEO and other persons having authority and responsibility for planning, directing and controlling the activities of the bank.

[9] As defined in the Notice on Bank's Recovery plan
[10] As defined in the Notice on Bank's Recovery plan
[11] As defined in the Notice on Pillar 3 - Public Disclosure Requirements, as may be revised from time to time

APPENDIX 1

LOSS EVENT TYPE CLASSIFICATION

Event-Type Category (Level 1)	Definition	Categories (Level 2)	Activity Examples (Level 3)
Internal Fraud	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.	Unauthorized Activity	• Transactions not reported (intentional) • Transaction type unauthorized (with 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 takeover/impersonation/etc. • Tax non-compliance/evasion (wilful) • Bribes/kickbacks • Insider trading (not on firm's account]
External fraud	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 • Credit Fraud
		Systems Security	• Hacking damage • Theft of information (with 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 • Organized labour activity
		Safe Environment	• General liability (slip and fall, etc.) • Employee health and safety rules events • Workers compensation
		Diversity and 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 requirements), or	Suitability, Disclosure and 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
		Improper Business	• Antitrust

Event-Type Category (Level 1)	Definition	Categories (Level 2)	Activity Examples (Level 3)
	from the nature or design of a product.	or Market Practices	• Improper trade/market practices • Market manipulation • Insider trading (on firm's account) • Unlicensed activity • Money laundering
		Product Flaws	• Product defects (unauthorized, etc.) • Model errors
		Selection, Sponsorship and 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 and Process Management	Losses from failed transaction processing or process management, from relations with trade counterparties and vendors.	Transaction Capture, Execution and 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 misperformance • Miscellaneous non-client counterparty disputes
		Vendors and suppliers	• Outsourcing • Vendor disputes

APPENDIX 2

Examples of tools used for identifying and assessing operational risk:

(a) Operational risk event data – Banks often maintain a comprehensive operational risk event dataset that collects all material events experience by the bank and serves as basis for operational risk assessments. The event dataset typically includes internal loss data, near misses, and, when feasible, external operational loss event data (as external data is informative of risks that common across the industry). Event data is typically classified according to a taxonomy defined in the ORMF policies and consistently applied across the bank. Event data typically includes date of the event (occurrence date, discovery date, and accounting date) and, in the case of loss events, financial impact. When other root cause information for events is available, ideally it can also be included in the operational risk dataset. When feasible, banks are encouraged to also seek to gather external operational risk event data and use this data in their internal analysis, as external is often informative of risks that are common across the industry.

(b) Self-assessments – Banks often perform self-assessments of their operational risks and controls on various different levels. The assessments typically evaluate inherent risk (the risk before controls are considered), the effectiveness of the control environment, and residual risk (the risk exposure after controls are considered) and contain both quantitative and qualitative elements. The qualitative element reflects consideration of both the likelihood and consequence of the risk event in the bank's determination of its inherent and residual risk ratings. The assessments may utilise business process mapping to identify key steps in business processes, activities, and organisational functions, as well as the associated risks and areas of control weakness. The assessments contain sufficiently detailed information on the business environment, operational risks, underlying causes, controls and evaluation of control effectiveness to enable an independent reviewer to determine how the bank reached its ratings. A risk register can be maintained to collate this information to form a meaningful view of the overall effectiveness of controls and facilitate oversight by senior management, risk committees, and the board.

(c) Event management – When banks experience an operational risk event, the process of identification, analysis, end-to-end management and reporting of the event follows a pre-determined set of protocols. A sound event management approach typically includes analysis of events to identify new operational risks, understand the underlying causes and control weaknesses, and formulate an appropriate response to prevent recurrence of similar events. This information is an input to the self-assessment and, in particular, to the assessment of control effectiveness.

(d) Control monitoring and assurance framework – Incorporating an appropriate control monitoring and assurance framework facilitates a structured approach to the evaluation, review and ongoing monitoring and testing of key controls. The analysis of controls ensures these are suitably designed for the identified risks and operating effectively. The analysis should also consider the sufficiency of control coverage, including adequate prevention, detection and response strategies. The control monitoring and testing should be appropriate for the different operational risks and key controls across business areas.

(e) Metrics – Using operational risk event data and risk and control assessments, banks often develop metrics to assess and monitor their operational risk exposure. These metrics may be simple indicators, such as event counts, or result from more sophisticated exposure models when appropriate. Metrics provide early warning information to monitor ongoing performance of the business and the control environment, and to report the operational risk profile. Effective metrics clearly link to the associated operational risks and controls. Monitoring metrics and related trends

through time against agreed thresholds or limits provides valuable information for risk management and reporting purposes.

(f) Scenario Analysis - Scenario analysis is a method to identify, analyse and measure a range of scenarios, including low probability and high severity events, some of which could result in severe operational risk losses. Scenario analysis typically involves workshop meetings of subject matter experts including senior management, business management and senior operational risk staff and other functional areas such as compliance, human resources and IT risk management, to develop and analyse the drivers and range of consequences of potential events. Inputs to the scenario analysis would typically include relevant internal and external loss data, information from self-assessments, the control monitoring and assurance framework, forward-looking metrics, root-cause analyses and the process framework, where used. The scenario analysis process could be used to develop a range of consequences of potential events, including impact assessments for risk management purposes, supplementing other tools based on historical data or current risk assessments. It could also be integrated with disaster recovery and business continuity plans, for use within testing of operational resilience. Given the subjectivity of the scenario process, a robust governance framework and independent review are important to ensure the integrity and consistency of the process.

(g) Benchmarking and comparative analysis - Benchmarking and comparative analysis are comparisons of the outcomes of different risk measurement and management tools deployed within the bank, as well as comparisons of metrics from the bank to other firms in the industry. Such comparisons can be performed to enhance understanding of the bank's operational risk profile. For example, comparing the frequency and severity of internal losses with self-assessments can help the bank determine whether its self-assessment processes are functioning effectively. Scenario data can be compared to internal and external loss data to gain a better understanding of the severity of the bank's exposure to potential risk events.

- END -