BANK NEGARA MALAYSIA
CENTRAL BANK OF MALAYSIA

Operational Risk

Applicable to:
1. Licensed banks
2. Licensed investment banks
3. Licensed Islamic banks
4. Licensed international Islamic banks
5. Licensed insurers
6. Licensed takaful operators
7. Licensed international takaful operators
8. Prescribed development financial institutions

Issued on: 10 May 2016 BNM/RH/PD 028-15

PART A OVERVIEW

1. Introduction

1.1 Operational risk refers to the risk of loss resulting from inadequate or failed internal processes, people and systems, or from external events. Operational risk is inherent in all activities, products and services of financial institutions and can transverse multiple activities and business lines within the financial institutions. It includes a wide spectrum of heterogeneous risks such as fraud, physical damage, business disruption, transaction failures, legal and regulatory breaches[1] as well as employee health and safety hazards. Operational risk may result in direct financial losses as well as indirect financial losses (e.g. loss of business and market share) due to reputational damage.

1.2 Over recent years, significant changes have been observed in the operational risk profile of financial institutions due to a number of factors including increased business complexity, greater regional expansion, more extensive outsourcing arrangements, faster staff turnover, greater reliance on technology and strengthened regulations. These factors have led to heightened inherent operational risks in financial institutions, with associated implications for operational risk management practices.

1.3 This policy document sets out the Bank's expectations for the management of operational risk by financial institutions. It aims to strengthen the governance, framework and processes for managing operational risk within financial institutions. Emphasis is also given to effective coordination in the management of operational risk with that of other risks (e.g. credit and market risks) to provide a holistic and integrated approach to a financial institution's overall risk management strategy.

1.4 For larger and more complex institutions, the policy document also addresses the need for greater scrutiny at business and functional lines given the higher inherent operational risks faced and the potential dilution of operational risk issues at board and senior management level. Robust operational risk management and oversight arrangements at the level of business and functional lines are therefore expected for the larger and more complex institutions.

2. Applicability

2.1 This policy document is applicable to all financial institutions as defined in paragraph 5.2.

[1] Including fiduciary breaches and Shariah non-compliance by Islamic financial institutions.

2.2 Notwithstanding paragraph 2.1:
(a) paragraph 7.6 is only applicable to an active financial market player as defined in paragraph 5.2; and
(b) paragraphs 8.5 and 8.6 are only applicable to an active financial market player and a large financial institution as defined in paragraph 5.2.

3. Legal provisions

3.1 The requirements of this policy document are specified pursuant to:
(a) sections 47(1) and 266 of the Financial Services Act 2013 (FSA);
(b) sections 57(1) and 277 of the Islamic Financial Services Act 2013 (IFSA); and
(c) sections 41(1) and 126 of the Development Financial Institutions Act 2002 (DFIA).

4. Effective date

4.1 This policy document comes into effect:
(a) One year from the date of issuance for financial institutions conducting banking business and Islamic banking business under FSA and IFSA respectively;
(b) One year from the date of issuance for prescribed development financial institutions providing credit and financing facilities under DFIA; and
(c) Two years from the date of issuance for financial institutions conducting insurance and takaful business under FSA and IFSA respectively.

5. Interpretation

5.1 The terms and expressions used in this policy document shall have the same meanings assigned to them in the FSA, IFSA or DFIA, as the case may be, unless otherwise defined in this policy document.

5.2 For purposes of this policy document:

"S" denotes a standard, an obligation, a requirement, specification, direction, condition and any interpretive, supplemental and transitional provisions that must be complied with. Non-compliance may result in enforcement actions;

"G" denotes guidance which may consist of statements or information intended to promote common understanding and advice or recommendations that are encouraged to be adopted;

"Board" means the board of directors of a financial institution, including a committee of the board where the responsibilities of the board set out in this policy document have been delegated to such a committee;

"senior management" refers to the chief executive officer and senior officers of a financial institution;

"financial institution" refers to:
(a) a licensed bank, licensed investment bank, and licensed insurer under the FSA;
(b) a licensed Islamic bank, licensed international Islamic bank, licensed takaful operator and licensed international takaful operator under the IFSA; and
(c) a prescribed development financial institution under the DFIA;

"active financial market player" refers to:
(a) a financial institution that is a major or key financial market participant as represented by its asset holdings, trading activities or risk exposures; or
(b) a financial institution that performs critical functions in the ongoing operation of the financial markets (such as clearing, payment, settlement and custodial agents);

"large financial institution" refers to:
(a) a financial institution with one or more business lines that are significant in terms of market share in the relevant industry; or
(b) a financial institution with a large network of offices within or outside the country through operations of branches and subsidiaries.

6. Related legal instruments and policy documents

6.1 This policy document must be read together with the following policy documents issued by the Bank:
(a) Policy Document on Risk Governance;
(b) Policy Document on Operational Risk Reporting Requirement – Operational Risk Integrated Online Network (ORION);
(c) Policy Document on Compliance;
(d) Guidelines on Introduction of New Products;
(e) Guidelines on Outsourcing;
(f) Guidelines on Management of IT Environment;
(g) Guidelines on Business Continuity Management; and
(h) Shariah Governance Framework.

PART B POLICY REQUIREMENTS

7. Board oversight

S 7.1 The Board must be aware of and understand the major operational risks in the financial institution's business and operating environment that could significantly impede the financial institution's ability to meet its obligation towards customers and counterparties, as well as those that could threaten the financial institution's safety and soundness. This would include risks arising from transactions or relationships with third parties, vendors and suppliers[2].

S 7.2 The Board must be conversant in both the financial and non-financial impact of all major operational risks to which the financial institution is exposed such as the impact arising from legal liability, loss of recourse, restitution, write downs, business interruption and reputational damage.

S 7.3 The Board must receive assurance that all key interdependencies between business and functional lines[3] are identified and ensure that it has a good understanding of the inter-relationship between operational risk and other financial and non-financial risks[4]. In particular, the Board must recognise and understand how operational risks affect the management of other financial and non-financial risks, and *vice versa*.

S 7.4 The Board must approve the operational risk appetite of the financial institution. In doing so, the Board must consider the financial institution's inherent operational risks, its financial condition, its current and future business direction, the quality of its internal control environment, and the institution's enterprise-wide risk management framework.

S 7.5 The Board must periodically review and affirm the operational risk appetite to ensure that it remains appropriate on an on-going basis.

S 7.6 In respect of an active financial market player, the Board must ensure that the operational risk appetite must specifically consider and address all major operational risks associated with the financial market activities that the institution is involved in[5].

G 7.7 The operational risk appetite and the financial institution's framework for identifying and assessing major operational risks should be coherent. This can be achieved by utilising information from the operational risk management

---

[2] Suppliers include outsourcing service providers. Specific requirements on outsourcing management are set out in the Guidelines on Outsourcing.

[3] Such as Human Resource, Finance and Information Technology.

[4] Including but not limited to credit, market, liquidity, Shariah non-compliance and insurance risks.

[5] Financial market activities could result in severe financial losses and reputation damage to financial institutions due to the high value, volume and velocity of the transactions, complexity of financial market instruments and the inter-dependencies among financial market participants, service providers and infrastructure.

tools, use of a common operational risk taxonomy and the consistent application of risk impact rating scales[6].

S 7.8 The operational risk appetite must include clearly defined limits for controlling the level of risk-taking within the operational risk appetite set by the Board. The limits set can be expressed in monetary or non-monetary terms[7] depending on the financial institution's business and operating environment.

G 7.9 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.

S 7.10 The Board must oversee the design and implementation of the operational risk management framework for the financial institution.

S 7.11 The operational risk management framework must provide for:

(a) appropriate governance and oversight structures, reporting lines and accountabilities for managing operational risk;
(b) sound approaches to operational risk identification, assessment, monitoring and reporting that utilises appropriate operational risk management tools;
(c) approved risk mitigation strategies and instruments for keeping risks within the limits set;
(d) clear definitions of operational risk and operational risk loss that are supported by a common operational risk taxonomy[8] to facilitate the consistent identification of operational risks across the organisation and an integrated reporting of operational risk;
(e) clear descriptions of risk limits and risk impact measures that correspond to the financial institution's approved operational risk appetite;
(f) the periodic review of the framework, policies and methodologies at regular intervals or whenever there are material changes in the financial institution's operational risk profile; and
(g) the regular independent review of the framework by the internal audit function.

S 7.12 The operational risk management framework must cover all businesses and functions of the financial institution, including those that are outsourced to

---

[6] Risk impact rating scales would assist in segregating risks that are within, that are reaching or that have breached the risk tolerance level. Risk impact rating scales may be defined in quantitative and/or qualitative terms. While quantitative rating scales (e.g. financial impact ratings) bring a greater degree of precision and measurability, qualitative descriptions are needed when the risks do not lend themselves to quantification.

[7] Non-monetary measures may be more appropriate to express the business objectives such as preserved reputation and business continuity. Examples of such measures are duration of negative publicity in the media and duration of system downtime.

[8] This should include the operational risk event types and causal categories.

external parties.

S 7.13 The operational risk management framework must be well integrated with other related risk management processes of the financial institution. In particular, the Board must ensure that the operational risk management framework addresses interactions between the financial institution's processes for managing the components of operational risks[9] so as to ensure a comprehensive and consistent approach to identify and profile operational risks in the financial institution.

S 7.14 For financial institutions that offer Islamic products and services, the Board must consider the unique operational risks that may arise due to Shariah non-compliance. This includes the financial and non-financial implications when the established Shariah requirements and rulings are not effectively communicated, translated into internal policies or observed by the financial institution across different business and functional lines[10].

S 7.15 The Board must ensure that it receives adequate information on material developments in the operational risk profile of the financial institution, including pertinent information on current and emerging operational risk exposures and vulnerabilities and on the effectiveness of the operational risk management framework. This must be supported by a robust and reliable operational risk information and monitoring system.

8. Senior management

S 8.1 Senior management is responsible for establishing policies, processes and limits for managing operational risks. These must be consistent with the risk appetite approved by the Board and implemented for all material products, activities, processes and systems across the financial institution.

S 8.2 Senior management must ensure that responsibilities for the effective implementation and maintenance of operational risk management policies, processes and limits are clearly set out and supported by effective reporting and escalation procedures.

S 8.3 The responsibilities for operational risk management must reside with business and functional lines as well as control functions. Senior management must ensure that business and functional lines are held responsible for the identification, assessment, mitigation and review of operational risk for specific products, activities, processes and systems within their purview. Appropriate authority must be given to staff who are responsible for operational risk management activities. Adequate resources must also be made available to support the staff in discharging their responsibilities.

---

[9] Such as technology, compliance and Shariah non-compliance risks.

[10] In addition, for financial institutions that offer both conventional and Islamic products and services, or Islamic financial institutions that adopt an operating model with shared services, operational risks arising from the use of common resources and systems also need to be considered.

S 8.4 Senior management must ensure effective arrangements at the senior management level are in place to oversee the financial institution's operational risk exposures and ensure the robust implementation of the operational risk management framework at the enterprise-wide level. Such arrangements must allow for the effective deliberation by senior management of operational risk issues at the enterprise-wide level, facilitate coordination with the financial institution's management of other risks and support senior management's ongoing review of the adequacy of the financial institution's operational risk management framework, including its implementation within significant businesses and functional lines.

S 8.5 An active financial market player or a large financial institution must additionally put in place appropriate oversight arrangements that focus on operational risk issues at significant business and functional lines to support the enterprise-wide oversight of operational risk. These arrangements must also provide for designated resources within the significant business and functional lines who are also responsible for undertaking the functions set out in paragraph 8.3 and who do not engage in risk taking activities.

G 8.6 In relation to paragraph 8.5, the arrangements at business and functional lines should allow for detailed deliberations of operational risk issues, provide business-specific focus on the implementation of operational risk management activities and support more effective day-to-day monitoring of major operational risks by staff with relevant business-specific expertise. Financial institutions may establish a committee or set up an embedded risk function for this purpose, or leverage on existing arrangements that have a similar focus on identifying and managing operational risk within the business and functional line.

G 8.7 The Bank may require a financial institution that is not an active financial market player or a large financial institution as defined in this document to apply the standards in paragraph 8.5 where the Bank assesses that the financial institution's operational risks are not adequately addressed by existing arrangements within the institution.

S 8.8 The coordination between the senior management oversight of operational risks at the enterprise-wide level and the oversight and operational risk management functions at each significant business or functional line must be clearly defined.

9. Enterprise-wide operational risk management function

S 9.1 An independent enterprise-wide operational risk management function[11] that reports to the Chief Risk Officer (CRO) must be made primarily responsible for the design, implementation, and on-going maintenance of an effective and

[11] This refers to independent risk management function outlined in Principle 7 of the Risk Governance policy document. An illustration of the structure and inter-relationship between the operational risk management function and an embedded operational risk function is provided in **Appendix 1**.

consistent enterprise-wide operational risk management framework. The responsibility of the function includes communicating the operational risk management policies, processes and limits throughout the organisation and facilitating the consistent implementation of these policies, processes and limits as well as validating compliance with the approved operational risk management framework across all business and functional lines.

S 9.2 The enterprise-wide operational risk management function does not substitute the primary role of business and functional lines in managing operational risk. However, it must be responsible for reviewing the identification and management of major operational risks by business and functional lines as well as integrating operational risks at the enterprise level. An important part of this process includes constructively challenging assessments produced by the business and functional lines and evaluating the effectiveness of the risk mitigation activities.

S 9.3 The CRO must also ensure that the operational risk management function does not operate in silo but coordinates and communicates effectively with the financial institution's other risk management and control functions[12].

S 9.4 The CRO must ensure that operational risk information reported to the Board and senior management is timely, relevant and presented in a manner that focuses their attention on important operational risk developments and supports informed and sound decisions.

10. Internal audit review

S 10.1 The internal governance structure must provide for regular reviews and assessments of the operational risk management framework, processes and systems by internal audit. The review by internal audit must include an assessment of the effectiveness of risk management activities undertaken by business and functional lines and the enterprise-wide operational risk management function, the effectiveness of senior management oversight of operational risks and whether the operational risk management framework remains comprehensive, robust and has been implemented as intended.

S 10.2 The results of the internal audit review must be effectively communicated to the Board and senior management. The Board and senior management must in turn ensure that appropriate and timely actions are taken to address any internal audit findings and maintain an effective operational risk management framework.

[12] Such as credit, market, liquidity, Shariah non-compliance and insurance risk management as well as compliance and internal audit functions.

11. Sound internal control environment

S 11.1 A financial institution must establish policies, procedures and systems that ensure a sound internal control environment. The internal control activities and processes must be commensurate with the financial institution's operational risk profile.

S 11.2 The internal control systems must support the effective control of operational risks at multiple stages and layers within a business process to provide adequate defence against a breakdown in controls at any stage or layer.

G 11.3 The provision of controls at multiple stages and layers within a business process is also described as '*defence in depth*'. '*Defence in depth*' is a concept in which multiple layers of internal controls are placed within a business process to prevent, detect or reduce the impact of a process breakdown in case any of the internal controls are compromised. When applying this concept, a financial institution should balance the strength of the embedded internal controls against the associated level of operational risk exposures.

S 11.4 The internal control systems must provide for the effective ongoing oversight of business activities at all operating levels of a financial institution, with clearly defined reporting responsibilities for all staff. A financial institution must ensure that there are no gaps in reporting lines that may enable individuals to conceal unauthorised actions and material errors or losses.

S 11.5 A financial institution must identify and minimise areas of potential conflicts and ensure that critical areas of operations are subjected to appropriate segregation of duties, dual control and independent monitoring.

S 11.6 A financial institution must ensure that both preventive and detective controls, are effectively deployed to respectively, prevent errors and irregularities from occurring and detect errors and irregularities that may have occurred.

G 11.7 The preventive and detective controls may include the following:

Preventive

(a) documented policies and procedures with clearly established authority and processes for approval;
(b) safeguards for access to, and use of, assets and records;
(c) on-going processes to identify business lines or products where returns appear to be out of line with reasonable expectations; and
(d) requirements for employees in roles that have high inherent operational risk to be on mandatory 'block' leave.

Detective

(a) enforcement and monitoring of assigned risk limits; and
(b) regular and ad-hoc verification and reconciliation of transactions and accounts.

S 11.8 A sound technology risk management framework[13] must be implemented to mitigate operational risks that may arise from compromised system and data integrity, security and performance. A financial institution must also ensure that its information technology infrastructure is able to support current and long term business requirements under normal as well as stressed operating conditions. An assessment of the adequacy of the financial institution's information technology infrastructure must be undertaken before material changes to the financial institution's business strategy are pursued.

S 11.9 A financial institution must monitor and regularly evaluate its internal control systems to ensure that they are operating effectively and to take account of changes in internal and external conditions. Enhancements must be made to these systems to address identified gaps and maintain their effectiveness.

S 11.10 The evaluation of internal control effectiveness must include established processes for:

(a) transaction sampling to test the level of compliance with internal policies and procedures;
(b) reviewing the treatment and resolution of instances of non-compliance;
(c) affirming that the required approvals and authorisations are assigned to an appropriate level of management; and
(d) analysing reports of approved exceptions to the limits, management overrides and other deviations from policy.

12. Identification and assessment of operational risks

S 12.1 A financial institution must have in place robust processes for the identification and assessment of operational risks that considers both internal and external factors and is comprehensive in its approach. The process must also facilitate effective risk management activities by identifying potentially significant operational risk events through the use of scenario analysis.

G 12.2 A sound operational risk identification and assessment methodology should be able to identify the internal and external risk drivers that influence key business objectives and strategies, evaluate and test the effectiveness of existing internal control systems and risk mitigants, and be sufficiently granular such that the institution is able to determine the root cause of a particular operational risk event.

G 12.3 The identification and assessment of operational risks should consider the following key inputs:

(a) management's knowledge of the current and future outlook of business and operating conditions and anticipated changes in products, processes, regulations and markets;

[13] Detailed requirements on technology risk management framework including related governance arrangements are as per the Guidelines on Management of IT Environment.

(b) operational risk exposures or internal control deficiencies identified by internal audit and other control functions or by regulators;
(c) business process mappings that identify the key steps, as well as risk (including risk interdependencies) and control points in business processes;
(d) operational risk indicators that capture the main drivers of operational risk exposures;
(e) historical internal loss experience and root-cause analyses of significant operational risk events; and
(f) analysis of relevant external loss information i.e. information on significant losses experienced by other organisations, where available.

S 12.4 A financial institution must combine both top-down and bottom-up approaches in its operational risk identification and assessment methodology.

G 12.5 A top-down approach to operational risk identification and assessment can help a financial institution to identify major operational risks that could undermine the soundness of the financial institution, whereas the bottom-up approach ensures comprehensiveness and promotes risk ownership and accountability. The use of both approaches allows financial institutions to validate the enterprise-wide level view of operational risks and to prioritise resources towards managing the major operational risks within the key business and functional lines.

S 12.6 The operational risk identification and assessment methodology must remain current, reflective of the dynamic nature of the financial institution's business and be aligned with the time horizon of the financial institution's business strategies and operational risk appetite[14]. The methodology must also be updated as and when there are major operational risk events or developments that could invalidate earlier assessments.

S 12.7 For scenario analysis, a financial institution must develop plausible scenarios under which the identified major operational risks could materialise. For each scenario, the financial institution must evaluate the effectiveness of the current controls and risk mitigants, identify the circumstances under which the controls and risk mitigants could fail, and estimate the probability of occurrence and severity of impact of an operational risk failure, including under a potential worst case scenario.

S 12.8 The scenario analysis must be supported by a robust methodology and process which incorporates inputs from business and functional lines, risk managers, subject matter experts[15] and key control functions[16]. Assumptions

[14] For example, if the outlook for capital planning is one year, operational risk identification and assessment must have a forward-looking time horizon of at least one year. However, given that the business and operating environment is dynamic and could rapidly change, the assessment may need to be updated more frequently e.g. half-yearly.
[15] The subject matter experts can be internal or external to the institution.
[16] The key control functions include risk management, compliance and internal audit functions.

used must be regularly reviewed. The methodology and process must be documented and approved by senior management and applied consistently.

G 12.9 In identifying the potential scenarios, financial institutions should consider events that may pose significant threat to the institution from an operational risk perspective such as new business ventures, corporate restructuring exercises, major IT projects and significant changes in product design and client management strategies. The potential scenarios may also be developed based on past incidences or loss experience of the financial institution. While stress testing can provide a complementary tool to identify potentially significant operational risk events, financial institutions should also consider other plausible scenarios including those incorporating multiple high frequency low impact events that could pose a significant threat if they occur concurrently.

13. Operational risk response and mitigation strategies

S 13.1 A financial institution must ensure that the operational risk mitigation strategies and responses effectively address all identified major operational risks in line with the operational risk appetite set by the Board.

S 13.2 When devising mitigation strategies, a financial institution must consider the impact of the mitigation strategies on other risks and whether the strategies adopted could introduce new risks to the financial institution, or create unintended effects on risk-taking incentives or on business and operational performance. The financial institution must ensure that these implications are clearly identified and effectively addressed in the financial institution's overall risk management framework.

S 13.3 Insurance and takaful arrangements can be useful to complement the management of operational risks, but they are not a substitute for a sound internal control environment. Where such arrangements are used, a financial institution must assess any residual risks and new risks that may arise, including an assessment of:

(a) the financial strength of the insurance or takaful provider and its ability to honour the insurance or takaful claim;
(b) the potential legal risk that may arise from the insurance policy or takaful contract;
(c) the potential liquidity risk that may arise due to the timing of insurance or takaful compensation payments; and
(d) the level of deductibles specified in the insurance policy or takaful certificate.

G 13.4 A financial institution should also consider the limitations of using insurance or takaful arrangements as a risk mitigation strategy, taking into account operational risk interdependencies that can change over time, quantification challenges as well as gaps between the actual operational risk exposure and the scope of insurance coverage.

S 13.5 A financial institution must be able to demonstrate that the risk mitigation strategies and responses can contain operational risk exposures of the financial institution within the operational risk appetite set by the Board. This must be supported by a regular assessment of trends in the financial institution's operational risk exposures and a process for affirming that the risk mitigation strategies and responses remain appropriate.

S 13.6 A financial institution must establish business continuity plans that are commensurate with its operational risk profile and the approved risk tolerance level towards business disruptions. The financial institution's business continuity plans must cover all critical business operations and address plausible business disruption events or scenarios associated with these operations[17].

14. Operational risk indicators, metrics and loss events

S 14.1 A financial institution must establish processes for monitoring operational risk exposures that include the systematic collection and analysis of relevant operational risk data and metrics.

S 14.2 Operational risk indicators and metrics must be able to support the early identification of emerging risks and potential changes to the financial institution's operational risk profile well in advance of the risks materialising. Accordingly, there must be appropriate limits set for each indicator to trigger appropriate escalation and mitigation actions.

S 14.3 The key operational risk indicators and metrics must include:

(a) generic indicators that are comparable across different business and functional lines and can be aggregated on an enterprise-wide basis e.g. staff turnover rate, mandatory leave utilisation, system downtime and compliance breaches; and

(b) customised indicators that monitor specific operational risks within individual business lines and processes e.g. reconciliation breaks, service level breaches, trade errors and transaction amendments and cancellations.

S 14.4 A financial institution must be able to capture and track actual operational risk loss events and near misses. This includes incidences of Shariah non-compliance for Islamic finance operations and operational risk-related events that lead to losses in other risk types e.g. credit, market and insurance risk.

S 14.5 A financial institution must ensure that operational risk loss events being tracked and monitored are complete and accurate by establishing the framework, processes and controls for collecting and reporting operational risk loss events. This must include a internal standard for loss recognition (e.g. to

[17] Detailed requirements on business continuity management are set out in the Guidelines on Business Continuity Management.

ascertain direct and indirect financial losses) that is consistently used, criteria for allocating losses arising from centralised functions or activities that span more than one business line as well as requirements for quantified losses to be validated against and reconciled with accounting records and other internal information.

15. Operational risk reporting

S 15.1 Operational risk reports to the Board and senior management must provide accurate information for decision making and facilitate timely management responses. The reporting frequency must therefore reflect the level of risks involved, as well as the pace and nature of changes in the business and operating environment.

S 15.2 Operational risk reports to the Board and senior management must contain financial, operational and compliance information, as well as external information about events and conditions that are relevant to decision making.

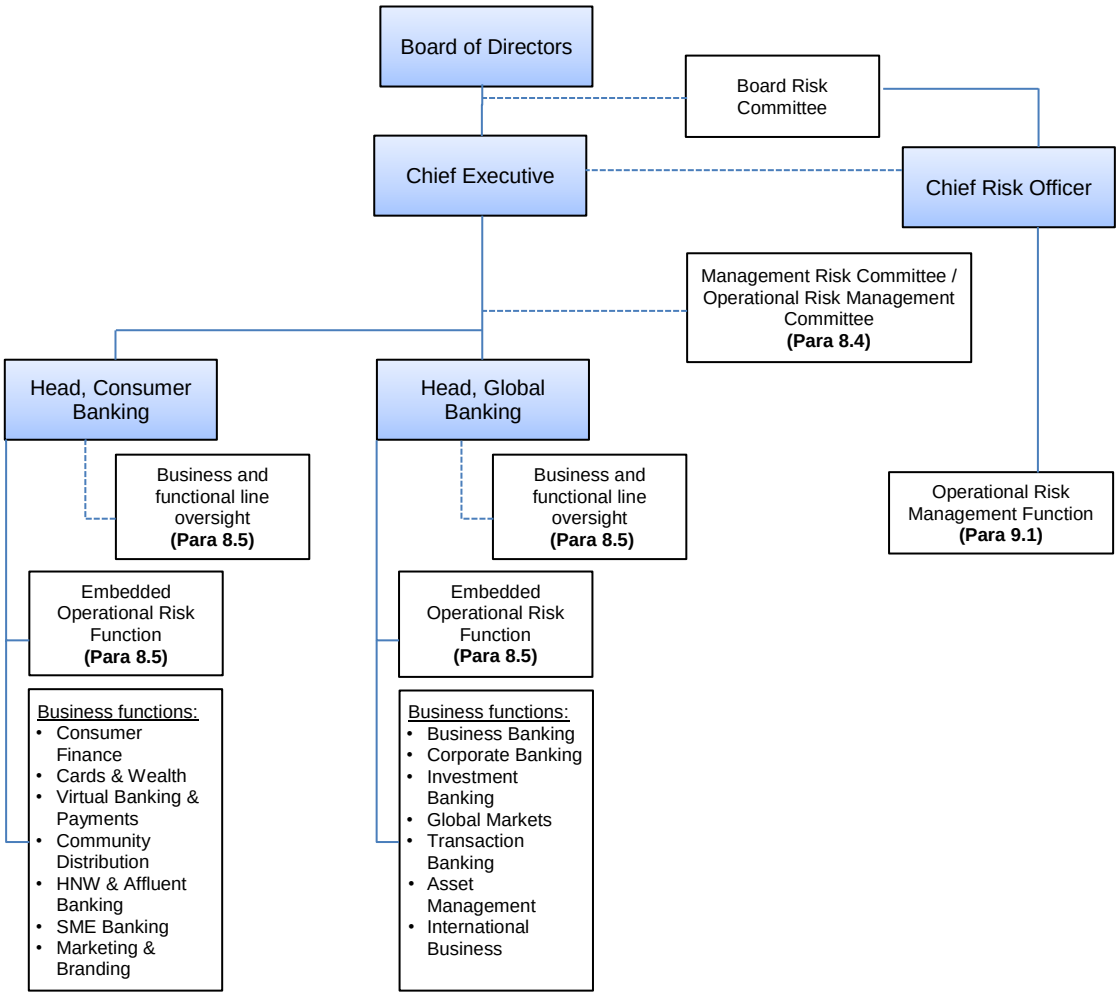
G 15.3 Operational risk information that could aid informed decision-making by the Board and senior management include:

(a) an analysis of the current operational risk profile, emerging trends of key operational risk indicators and the direction of the risks over a defined horizon (e.g. over the next three months);
(b) the status of mitigation action plans for material operational risks;
(c) breaches of operational risk limits, in particular those resulting in the financial institution's enterprise-wide operational risk level being higher than the approved risk appetite;
(d) observations of operational risk management deficiencies by the operational risk management function, internal audit or regulators;
(e) significant operational risk events, control failures and losses that have occurred; and
(f) lessons learnt from relevant external loss events and internal assessments of the probability and potential impact of similar events occurring in the financial institution.

S 15.4 The scope, context and level of granularity of operational risk reports must be appropriately tailored to the needs of the different groups of users of the reports.

G 15.5 For example, detailed operational risk information specific to activities and operations of the business and functional lines is appropriate and useful to the business and functional line management, whereas a high-level overview of the overall operational risk profile of the financial institution and executive summaries of significant enterprise-level operational risks would be more beneficial to facilitate decision-making by the Board and senior management.

APPENDIX 1 – EXAMPLE OF AN OPERATIONAL RISK GOVERNANCE MODEL FOR ACTIVE FINANCIAL MARKET PLAYERS AND LARGE FINANCIAL INSTITUTIONS



- Management Risk Committee's accountability includes the oversight of the enterprise-wide operational risk function. The Management Risk Committee may establish an Operational Risk Management Committee to ensure a more focused oversight on operational risk.
- Committees within the significant business and functional lines of the financial institution are entrusted with the responsibility to monitor and deliberate on operational risk issues specific to the business or functional lines, and promote risk ownership and management by the business and functional lines.
- The operational risk management function is responsible for the design and implementation of the enterprise-wide operational risk framework, policies and processes, as well as for validating and challenging the results of operational risk management activities of the business and functional lines.
- The embedded operational risk function, which is part of the business and functional line, would assist in implementing and monitoring the operational risk management activities within the business and functional lines. The embedded operational risk function's close relationship and knowledge of the business allows for more focused implementation and oversight.