Operational Risk Management
Concept Paper
PART A  Overview ........................................................................................................ 3
  1. Introduction ......................................................................................................... 3
  2. Policy objectives ................................................................................................. 3
  3. Applicability ....................................................................................................... 3
  4. Legal provisions .................................................................................................. 4
  5. Effective date ...................................................................................................... 4
  6. Interpretation ...................................................................................................... 4
  7. Related legal instruments and policy documents ................................................. 5

PART B  PRinciples for sound operational risk management.............................. 6
  8. Board oversight ................................................................................................... 6
  9. Role of senior management ................................................................................ 9
 10. Sound internal control environment .................................................................. 13
 11. Identification and assessment of operational risks .............................................. 15
 12. Operational risk response and mitigation strategies .......................................... 17
 13. Key operational risk indicators and metrics ....................................................... 19
 14. Operational risk reporting .................................................................................. 20

Appendix 1 – Example of Operational Risk Governance Model for Large Financial
Institutions .............................................................................................................. 22

Appendix 2 – Operational Risk Loss Event Type Classification.......................... 23
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.

2. Policy objectives

2.1 This policy document:
   a. sets out the Bank’s supervisory expectations with regard to the financial institution’s operational risk management framework and practices; and
   b. forms the basis for the Bank’s supervisory assessments of the effectiveness of an individual financial institution’s management of operational risks.

3. Applicability

3.1 The policy document is applicable to all financial institutions as defined in paragraph 6.2.

3.2 Notwithstanding paragraph 3.1:
   a. paragraph 8.5 is only applicable to an active financial market player as defined in paragraph 6.2;
   b. paragraphs 9.3 and 9.4 are only applicable to a large financial institution as defined in paragraph 6.2; and

\(^1\) Including fiduciary breaches and Shariah non-compliance by Islamic financial institutions.

Issued on: 27 June 2014
c. paragraph 9.8 is only applicable to a large financial institution or an active financial market player as defined in paragraph 6.2.

4. Legal provisions

4.1 The requirements of this policy document are specified pursuant to:
   a. sections 47(1), 56 and 266 of the Financial Services Act 2013 (FSA);
   b. sections 57(1), 65 and 277 of the Islamic Financial Services Act 2013 (IFSA); and

5. Effective date

5.1 This policy document comes into effect on DD MM 20XX.

6. Interpretation

6.1 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.

6.2 For purposes of this policy document:

   “S” denotes a standard, requirement or specification that must be complied with. Failure to comply may result in one or more enforcement actions;

   “G” denotes guidance which may consist of such information, advice or recommendation intended to promote common understanding and sound industry practices which are encouraged to be adopted;

   “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 and licensed takaful operator under the IFSA; and

c. a prescribed institution under the DFIA;

“active financial market player” refers to a financial institution that is a major or key participant, or an infrastructure/service provider (such as clearing, payment, settlement and custodial agents) in the capital, money, foreign exchange and derivative markets.

“large financial institution” refers to:

a. a financial institution with multiple sizeable businesses within the entity;

b. a financial institution with a large network of offices within or outside the country; or

c. a financial conglomerate with multiple sizeable entities within the corporate group.

7. Related legal instruments and policy documents

7.1 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. Guidelines on Introduction of New Products;

d. Guidelines on Outsourcing;

e. Guidelines on Management of IT Environment; and

PART B PRINCIPLES FOR SOUND OPERATIONAL RISK MANAGEMENT

8. Board oversight

Principle 1: The Board must be aware of and understand all major operational risks that could significantly impede the financial institution’s ability to meet its obligations towards customers and counterparties, as well as those that could threaten the financial institution’s safety and soundness. The Board must approve the financial institution’s operational risk appetite that sets out the tolerance towards the major operational risks and the strategies for managing risks within the tolerance limits.

8.1 The Board must be aware of and understand the nature and complexity of the major operational risks in its business and operating environment, including risks arising from transactions or relationships with third parties, vendors and suppliers. This should include an understanding of both the financial and non-financial impact of operational risk to which the financial institution is exposed such as the impact arising from legal liability, loss of recourse, restitution, write downs, business interruption and damage.

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

8.3 The Board must review and approve the operational risk appetite statement that covers all major operational risks that the financial institution is exposed to. In doing so, the Board must consider the financial institution’s level of risk aversion, its financial condition, its current and future business direction and the quality of its internal control environment.

---

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 and insurance risks.

Issued on: 27 June 2014
S 8.4 The risk appetite statement must include risk limits and thresholds approved by the Board for specific operational risks and an aggregate operational risk limit reflecting the financial institution’s tolerance towards operational risks. The risk limits must be consistent with management’s strategies for managing risks within the limits and thresholds set.

S 8.5 In respect of an active financial market player, the Board must ensure that the operational risk appetite statement includes all major operational risks associated with the financial market activities that the institution is involved in.

G 8.6 The operational risk limits and thresholds should reflect an appropriate combination of quantitative metrics as well as qualitative analysis of major operational risk exposures, taking into account conditions in the financial institution’s business and operating environment as well as factors that can increase operational risk exposures but which may not be adequately captured by quantitative measures. The Board should also consider limitations in operational risk measurement methodologies that are still evolving, and ensure that the operational risk limits and thresholds set appropriately address these limitations in order to effectively manage and contain exposures to operational risk.

**Principle 2:** The Board must oversee the design and implementation of a sound operational risk management framework and provide constructive challenge to senior management on the credibility and robustness of the policies, processes and systems for managing major operational risks.

S 8.7 The Board must ensure that the design and implementation of the financial institution’s operational risk management framework provides for:

a. a clear definition of operational risk and operational risk loss. This must be supported by a common operational risk taxonomy that includes the operational risk event types and causal categories to facilitate the consistent identification of operational risks across the organisation and the management of operational risk in an integrated manner;

---

5 Operational risk is one of the major risks in financial market activities that could result in severe financial losses and reputation damage to the 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.
b. appropriate governance and oversight structures, reporting lines and accountabilities for managing operational risk;

c. a clear description of risk limits, thresholds and risk impact rating scales\(^6\) that correspond to the financial institution’s approved operational risk appetite and tolerance;

d. the approved risk mitigation strategies and instruments for keeping risks within the thresholds and limits set;

e. a sound approach to operational risk identification, assessment, monitoring and reporting that utilises appropriate operational risk management tools;

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 8.8 The operational risk management framework must cover all businesses and functions of the financial institution, including those that are outsourced to external parties.

S 8.9 The operational risk management framework must be well integrated with other risk management processes of the financial institution. The Board must ensure in particular that the operational risk management framework addresses the inter-relationship between the framework and the financial institution’s processes for managing technology, compliance and Shariah risks so as to ensure a comprehensive and consistent approach to the identification and profiling of operational risks in the financial institution.

S 8.10 For financial institutions that offer Islamic products and services, the Board should be aware of the unique operational risks that may arise due to Shariah non-compliance such as the financial and non-financial implications when established Shariah requirements and rulings are not effectively communicated, translated into

---

\(^6\) Risk impact rating scales would assist in segregating risks that are within the risk tolerance, risks that are reaching the risk tolerance level and risks that have breached the risk tolerance level. 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.
internal policies or observed by the financial institution across different businesses and functional units. This is particularly relevant for a financial institution that offers both conventional and Islamic products and services, and adopts an operating model where common staff undertakes the sales, support and control functions for both conventional and Islamic products and services.

8.11 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 the current and emerging operational risk exposures and vulnerabilities and information on the effectiveness of the operational risk management framework. The Board must challenge the quality and comprehensiveness of the operational risk information it receives and be satisfied with the reliability of the financial institution’s operational risk information and monitoring system.

9. Role of senior management

Principle 3: The senior management must ensure effective implementation and maintenance of policies, processes and systems for managing operational risk in all material products, activities, processes and systems, consistent with the operational risk management framework and operational risk appetite and tolerance approved by the Board.

9.1 The senior management must translate the approved operational risk management framework into specific policies, processes and limits that can be implemented for all material products, activities, processes and systems across the financial institution. Responsibilities must be clearly set out for communicating these operational risk management policies, processes and limits throughout the organisation and ensuring their effective implementation and maintenance. This must be supported by the appropriate authority given to the staff carrying these responsibilities, effective reporting and escalation procedures and adequate resources to discharge their responsibilities.

9.2 Senior management must establish an effective platform (i.e. a senior management oversight body) for overseeing the financial institution’s operational
risk exposures and ensuring the robust implementation of the operational risk management framework and processes at the enterprise-wide level. Such a platform must allow for the effective deliberation by senior management of operational risk developments 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 programme, including its implementation within significant businesses and functional units.

S 9.3 In respect of a large financial institution, a dedicated sub-committee \(^7\) at each significant business or function must be established to support senior management in its enterprise-wide oversight of operational risks. The sub-committee must serve to provide a platform for more detailed deliberations of operational risk exposures and issues specific to the businesses or functions and input to senior management’s assessment of the financial institution’s overall management of operational risks at the enterprise-wide level.

S 9.4 The responsibilities of the dedicated sub-committees and the scope of operational risks covered by each sub-committee must be clearly defined. There must be clear arrangements established on how the sub-committees engage with and report to the senior management oversight body on their assessments of operational risks within significant businesses and functions.

S 9.5 Records kept by the senior management oversight body and sub-committees must be adequate to facilitate the review and evaluation of their effectiveness.

**Principle 4: Senior management must put in place an effective internal governance structure as approved by the Board for managing operational risks, with clearly defined accountabilities, roles, authority and reporting relationships that complement and mutually reinforce one another.**

\(^7\) An illustration of a possible governance structure and inter-relationship between the senior management committee and the sub-committees within the significant businesses and functions is provided in Appendix 1.
9.6 Business and functional line management is responsible for the identification and management of operational risks within its products, activities, processes and systems. The business and functional line management must establish and execute risk mitigation strategies and processes as approved by the Board and senior management of the financial institution, and ensure that internal controls are implemented effectively.

9.7 The business and functional line management must periodically review whether internal controls and operational risk mitigation strategies are working effectively to manage operational risks within the financial institution’s approved risk tolerance. There must be clear expectations and processes established to ensure prompt escalation and actions to address any gaps or issues identified.

9.8 In respect of a large financial institution or an active financial market player, an embedded operational risk function must be established within each significant business and functional line. The embedded operational risk function is responsible for implementing the operational risk management activities within the business and functional lines and undertakes detailed assessments, supported by credible data analytics, of the operational risks in the business and functional lines. Staff in the embedded operational risk function must not have responsibility for risk-taking activities in the business or functional lines.

9.9 The embedded operational risk function provides a business-specific focus on the implementation of operational risk management activities and supports more effective day-to-day monitoring of major operational risks. Given the inherent complexity and scale of operations of large financial institutions and active financial market players, the embedded operational risk function is considered to be sound practice to strengthen the management of operational risks by business and functional lines through a dedicated focus on operational risk management activities that are supported by relevant business-specific expertise.

9.10 A central operational risk management function that is independent of the business and functional line management and reports to the Chief Risk Officer

---

8 Including risks associated with the procurement of external services, insurance risk transfer and outsourcing arrangements.

9 An illustration of the structure and inter-relationship between the central operational risk management function and an embedded operational risk function is provided in Appendix 1.

Issued on: 27 June 2014
(CRO), must be made primarily responsible for the design, ongoing development and maintenance of an effective and consistent enterprise-wide operational risk management framework. This includes facilitating the consistent implementation of policies and processes for managing operational risks across all business and functional lines and validating compliance with the approved operational risk management framework.

9.11 The central operational risk management function must also be responsible for reviewing the identification and management of major operational risks by business and functional lines and integrating operational risks at the enterprise level. An important part of this process includes constructively challenging operational risk assessments produced by the business and functional lines (including the embedded operational risk function established within business and functional lines required under paragraph 9.8) and evaluating the effectiveness of risk mitigation activities.

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

9.13 Consistent with paragraph 8.9, the CRO must ensure that the central 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.

9.14 The internal governance structure must provide for regular independent reviews and assessments of the operational risk management framework, processes and systems by the internal audit function. The review by the internal audit function must include an assessment of the effectiveness of risk management activities undertaken by business and functional lines and the centralised 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.

---

10 Such as credit, market, liquidity, Shariah, insurance risk management, compliance and internal audit functions.
9.15 The results of the independent reviews by internal audit must be effectively communicated to senior management and the Board. The Board and senior management must in turn ensure that appropriate and timely actions are taken to maintain an effective operational risk management framework.

10. Sound internal control environment

Principle 5: 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.

10.1 A financial institution’s internal control systems must be designed to provide assurance of the integrity of the financial institution’s operations, including the safeguarding of its assets, reliability of financial reports and compliance with applicable laws and regulations as well as internal policies. These internal control systems should support the effective control of operational risks at multiple stages and layers within a business process to provide an adequate defence against a breakdown in controls at any stage or layer. A financial institution must be able to demonstrate that the strength of the overall internal control systems is commensurate with the financial institution’s operational risk exposures.

10.2 In providing controls at multiple stages and layers, financial institutions should avoid using similar control triggers at all stages to improve the probability of detecting a breach in internal controls or reducing impact of the breach in the event of a breakdown at any stage or layer. The design of layered controls should balance the complexity that this can add to operational processes against the associated level of operational risk impact to the financial institutions resulting from a breakdown in controls.

10.3 The internal control environment must be supported by the effective ongoing supervision 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 10.4** 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 10.5** A financial institution must ensure that both preventive and detective controls\(^{11}\), are effectively deployed. This includes:

a. documented policies and procedures with clearly established authorities and processes for approval;

b. enforcement and monitoring of assigned risk thresholds and limits;

c. safeguards for access to and use of assets and records;

d. on-going processes to identify business lines or products where returns appear to be out of line with reasonable expectations;

e. regular and ad-hoc verification and reconciliation of transactions and accounts; and

f. requirements for key officers and employees to be on mandatory ‘block’ leave.

**S 10.6** The use of information technology to support a financial institution’s products, activities and processes must be subject to a sound technology risk management framework and governance arrangements\(^{12}\) to mitigate operational risks that can arise from compromised system and data integrity, security and performance. A financial institution must further ensure that its information technology infrastructure meets current and long term business requirements by providing sufficient capacity for a normal level of activity as well as for periods of market stress. 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 10.7** A financial institution must monitor and regularly evaluate its internal control systems to ensure that they are operating effectively and to take account of

---

\(^{11}\) Preventive controls are designed to keep errors and irregularities from occurring, while detective controls are designed to detect errors and irregularities that may have occurred.

\(^{12}\) Detailed requirements on technology governance and information system infrastructure risk management programme are as per the Guidelines on Management of IT Environment.
changing internal and external conditions. Enhancements must be made to these systems to address identified gaps and maintain their effectiveness.

10.8 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 to ensure accountability are assigned to an appropriate level of management; and
   d. analysing reports of approved exceptions to thresholds and limits, management overrides and other deviations from policy.

11. Identification and assessment of operational risks

Principle 6: A financial institution must have in place a robust process 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.

11.1 The operational risk identification and assessment processes must have a strong focus on material operational risks and vulnerabilities that could significantly impede the financial institution’s ability to meet obligations towards customers and counterparties, or threaten the financial institution’s safety and soundness.

11.2 A sound operational risk identification and assessment methodology should be able to identify the critical success factors of the key business objectives and strategies, examine the risk drivers in both the internal and external environments, evaluate and test the effectiveness of existing internal control systems and risk mitigations, and be sufficiently granular so as to be able to determine the root causes that need to be treated and monitored.

11.3 In identifying and assessing operational risks, a financial institution must consider the following important information sources:

Issued on: 27 June 2014
a. management’s knowledge of the current and future outlook of business and operating conditions and anticipated changes in products, processes, regulation and markets;
b. the operational risk exposures or control deficiencies identified by internal audit, control functions or regulators;
c. business process mappings that identify the key steps, as well as risk (including risk interdependencies) and control points in business processes;
d. the key operational risk indicators that capture the main drivers of operational risk exposures;
e. the historical loss experience and root-cause analyses of significant operational risk events; and
f. the analysis of relevant external loss information (i.e. information on significant losses experienced by other organisations), where available.

**S 11.4** A financial institution must combine both top-down and bottom-up approaches in its operational risk identification and assessment programme.

**G 11.5** A top-down approach to operational risk identification and assessment can help a financial institution to identify priority areas and top operational risk concerns 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 businesses and activities.

**S 11.6** A financial institution must develop plausible scenarios under which the identified major enterprise-wide operational risks could materialise. For each scenario, the financial institution must evaluate the strengths and limitations of the current controls and risk mitigants, analyse the circumstances under which the controls and risk mitigants could fail, and estimate the probable rate of occurrence and severity of the impact of an operational risk failure, including under a potential worst case scenario.

**S 11.7** Given the subjectivity of scenario analysis, a financial institution must ensure that the analysis is well-supported by a methodology and process which involves
proper design and planning, inputs from business and functional lines, risk managers and expert assessors, independent challenge by the key control functions\(^{13}\) and the regular review of the assumptions used. The process must be documented and approved by the Board to ensure a consistent approach and integrity of the results of the scenario analysis.

11.8 Operational risk identification and assessment must remain current, reflective of the dynamic nature of the financial institution’s business and aligned with the time horizon of the financial institution’s business strategies and operational risk tolerance\(^{14}\). The operational risk identification and assessment must also be updated as and when there are major operational risk events or developments that could invalidate the earlier risk identification and assessments.

### 12. Operational risk response and mitigation strategies

**Principle 7:** 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 tolerance set by the Board.

12.1 A financial institution must devise and implement appropriate risk mitigation strategies and responses to address identified major operational risks in a timely manner. This may include strengthening internal controls, transferring residual risks through insurance and reinforcing business continuity management arrangements.

12.2 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 incentives or on business and operational performance. The financial

\(^{13}\) The key control functions include senior management, central operational risk management, compliance and internal audit functions.

\(^{14}\) For example, since 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 the dynamic changes in business and operating environment, the assessment may need to be updated at a more frequent interval (e.g. half-yearly).
institution must ensure that these implications are clearly identified and effectively addressed in the financial institution’s overall risk management framework.

**S 12.3** Insurance arrangements can be useful to complement the management of operational risks, but they are not a substitute for a sound internal control environment. Where insurance arrangements are used, a financial institution must assess the residual risks as well as new risks that arise, including an assessment of:

a. the financial strength of the insurance provider and the ability to honor the insurance claim;
b. the potential legal risk that may arise from the policy contract;
c. the potential liquidity risk that may arise due to the timing of insurance compensation payments; and
d. the level of deductibles for each major risk type.

**G 12.4** A financial institution should also consider the limitations of insurance as a risk mitigation strategy, taking into account operational risk interdependencies which can change over time, the quantification challenges as well as gaps between the actual operational risk exposure and the scope of insurance coverage.

**S 12.5** A financial institution must be able to provide a high degree of assurance that the risk mitigation strategies and responses can contain operational risk exposures of the financial institution within the operational risk tolerance of the Board. This must be supported by a regular assessment of trends in the financial institution’s operational risk exposures as identified under Principle 6 and a process for affirming that the risk mitigation strategies and responses remain appropriate.

**S 12.6** A financial institution must establish business continuity plans that are commensurate with its operational risk profiles and the approved risk tolerance 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\(^\text{15}\).

\(^{15}\) Detailed requirements on business continuity management are set out in the Guidelines on Business Continuity Management.

Issued on: 27 June 2014
13. Key operational risk indicators and metrics

Principle 8: A financial institution must establish processes for monitoring operational risk exposures that includes the systematic collection and analysis of relevant operational risk data and metrics.

S 13.1 A financial institution must identify and monitor key operational risk indicators and metrics that provide insights on the material operational risk exposures of the financial institution. The risk indicators and metrics must be able to alert those responsible for managing operational risks 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 thresholds and limits set for each indicator to trigger appropriate escalation and mitigation actions.

S 13.2 The key operational risk indicators and metrics must include:

a. generic indicators that are comparable across different business and functional units 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 units and processes (e.g. reconciliation breaks, service level breaches, trade errors, amendments and cancellations).

S 13.3 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 losses).

S 13.4 The systems employed for tracking and monitoring the operational risk loss events must conform to the internal operational risk event taxonomy and include relevant information such as date of the loss event, gross loss amount and recoveries, descriptive information about the loss event, its causes and drivers and remedial actions. The internal operational risk event taxonomy must be at least mapped to the Level 2 Category of the Operational Risk Loss Event Type Classification, as per Appendix 2.
S 13.5 A financial institution must ensure that the systems for tracking and monitoring operational risk loss events are complete and accurate by establishing the framework, processes and controls for collecting and reporting operational risk loss events. This must include a standard to be consistently adopted for loss recognition (e.g. to ascertain direct and indirect financial losses), criteria for allocating losses arising in centralised functions or activities that span more than one business lines as well as requirements for quantified losses to be validated against and reconciled with accounting records and other internal information.

14. Operational risk reporting

Principle 9: Operational risk reports to the senior management and Board must be comprehensive, accurate, timely and appropriately designed to facilitate effective communication and understanding of operational risk issues and decision-making.

S 14.1 Operational risk reports must facilitate timely management responses and decision making. The reporting frequency must therefore reflect the level of risks involved, as well as the pace and nature of changes in the operating and external environments.

S 14.2 Operational risk reports to the senior management and Board must contain financial, operational and compliance information, as well as external market or environmental information about events and conditions that are relevant to decision-making.

G 14.3 Examples of operational risk information that could aid informed decision-making by the senior management and Board include:
   a. an analysis of the current operational risk profile, the emerging trends and patterns of the 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 thresholds and limits, in particular those resulting in the financial institution’s enterprise-wide operational risk level being higher than the approved risk appetite and tolerance;
d. observations of operational risk management deficiencies by the central operational risk management function, internal audit or regulators;

e. highlights on significant operational risk events, control failures and losses; and

f. the 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 14.4 The scope, context and level of granularity of operational risk reports must be appropriately tailored for the different group of users of the reports.

G 14.5 For example, detailed operational risk information specific to activities and operations of the business and functional units 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 the senior management’s and Board’s decision-making process.
APPENDIX 1 – Example of Operational Risk Governance Model for Large Financial Institutions

- Management Risk Committee’s accountability includes the oversight of the enterprise-wide operational risk. The Management Risk Committee may establish an Operational Risk Management Committee to ensure a more focused oversight on operational risk.

- Business-level committees within the large businesses of the financial institution are entrusted with the responsibility to monitor and deliberate on operational risk issues specific to the business. This would reduce the load on the Management Risk Committee and promote risk ownership by the businesses.

- The Central Operational Risk Management function is responsible for the design and implementation of the enterprise-wide operational risk framework, policies and processes, as well as validating and challenging the results of operational risk management activities of the businesses.

- The embedded operational risk function, which is part of the business, would assist the business in implementing and monitoring the operational risk management activities within the business. The embedded operational risk function’s close relationship and knowledge of the business allows for more focused implementation and oversight.
APPENDIX 2 – Operational Risk Loss Event Type Classification

<table>
<thead>
<tr>
<th>Event-type Category (Level 1)</th>
<th>Categories (Level 2)</th>
<th>Activity Examples (Level 3)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internal Fraud</td>
<td>Unauthorised Activity</td>
<td>Transactions not reported (intentional)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Transaction type unauthorised (with monetary loss)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Mismatching of position (intentional)</td>
</tr>
<tr>
<td></td>
<td>Theft and Fraud</td>
<td>Fraud/ worthless deposits/ false insurance claims</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Theft/ extortion/ embezzlement/ robbery</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Misappropriation of assets/ insurance premium</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Malicious destruction of assets</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Forgery</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Smuggling</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Account take-over/ impersonation etc.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Tax non-compliance/ evasion (wilful)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Bribe/ kickbacks</td>
</tr>
<tr>
<td></td>
<td>Systems Security</td>
<td>Insider trading</td>
</tr>
<tr>
<td>External Fraud</td>
<td>Theft and Fraud</td>
<td>Theft/ fraud/ robbery</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Forgery/ counterfeit (Cover Notes, Policy Certificates, Currency, Cheque, Security Documents/Identification documents)</td>
</tr>
<tr>
<td></td>
<td>Systems Security</td>
<td>Hacking damage</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Theft of information</td>
</tr>
<tr>
<td>Employment Practices and Workplace Safety</td>
<td>Employee Relations</td>
<td>Compensation, benefit, termination issues</td>
</tr>
<tr>
<td></td>
<td>Safe Environment</td>
<td>Organised labour activity</td>
</tr>
<tr>
<td></td>
<td>Diversity and Discrimination</td>
<td>General liability (slip and fall, etc.)</td>
</tr>
<tr>
<td></td>
<td>Selection, Sponsorship and Exposure</td>
<td>Employee health &amp; safety rules events</td>
</tr>
<tr>
<td></td>
<td>Advisory Activities</td>
<td>Workers compensation</td>
</tr>
<tr>
<td>Clients, Products and Business Practices</td>
<td>Suitability, Disclosure and Fiduciary</td>
<td>Fiduciary breaches/ guideline violations</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Suitability/ disclosure issues (KYC, etc.)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Retail customer disclosure violations</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Breach of privacy</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Aggressive sales</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Account churning</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Misuse of confidential information</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Lender liability</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Mis-selling/ Mis-informing of Shariah contract</td>
</tr>
<tr>
<td></td>
<td>Improper Business or Market Practices</td>
<td>Antitrust/ Improper trade/ market practices</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Market manipulation</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Insider trading (on firm’s account)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Unlicensed activity</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Money laundering</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Poor servicing by agents</td>
</tr>
<tr>
<td></td>
<td>Product Flaws</td>
<td>Product defects (include Shariah non-compliance products)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Model errors</td>
</tr>
<tr>
<td></td>
<td>Selection, Sponsorship and Exposure</td>
<td>Failure to investigate client per guidelines</td>
</tr>
<tr>
<td></td>
<td>Advisory Activities</td>
<td>Exceeding client exposure limits</td>
</tr>
<tr>
<td>Damage to Physical Assets</td>
<td>Disasters and Other Events</td>
<td>Natural disaster losses</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Human losses from external sources (terrorism, vandalism)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Damage to inventory (Islamic finance-related)</td>
</tr>
<tr>
<td>Business Disruption and System Failures</td>
<td>Systems failure and disruption</td>
<td>Hardware</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Software</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Telecommunications</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Utility outage/ disruptions</td>
</tr>
<tr>
<td></td>
<td>Business disruption (non-system)</td>
<td>Business closure due to external sources (pandemic, civil unrest)</td>
</tr>
<tr>
<td>Execution, Delivery and Process Management</td>
<td>Transaction Capture, Execution and Maintenance</td>
<td>Miscommunication</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Data entry, maintenance or loading error</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Missed deadline or responsibility</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Model/ system mis-operation</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Accounting error/ entity attribution error</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Other task mis-performance</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Delivery failure</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Collateral management failure</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Reference Data Maintenance</td>
</tr>
<tr>
<td></td>
<td>Monitoring and Reporting</td>
<td>Failed mandatory reporting obligation</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Inaccurate external report (loss incurred)</td>
</tr>
<tr>
<td></td>
<td>Customer Intake and Documentation</td>
<td>Client permissions/ disclaimers missing</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Legal documents missing/ incomplete</td>
</tr>
<tr>
<td></td>
<td>Customer/ Client Account Management</td>
<td>Unapproved access given to accounts</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Incorrect client records (loss incurred)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Negligent loss or damage of client assets</td>
</tr>
<tr>
<td></td>
<td>Trade Counterparties</td>
<td>Non-client counterparty mis-performance</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Miscellaneous non-client counterparty disputes</td>
</tr>
<tr>
<td></td>
<td>Vendors and Suppliers</td>
<td>Outsourcing</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Vendor disputes</td>
</tr>
</tbody>
</table>

Issued on: 27 June 2014