Implementation of Operational Risk Management Framework

Issued under BPRD circular # 04 dated May 20, 2014

Banking Policy & Regulations Department

This page is left blank intentionally

The Team

Name	Designation
Muhammad Ashraf Khan	Executive Director Banking Policy and Regulation Group
Shaukat Zaman	Director Banking Policy & Regulations Department
Lubna Farooq Malik	Director Off-site Supervision & Enforcement Department
Syed Jahangir Shah	Senior Joint Director Banking Policy & Regulations Department
Ahsin Waqas	Joint Director Banking Policy & Regulations Department

For queries please contact syed.jahangir@sbp.org.pk or ahsin.waqas@sbp.org.pk

This page is left blank intentionally

Table of Contents

This page is left blank intentionally

Executive Summary

Banks in Pakistan are using Basic Indicator Approach or the standardized approaches for the calculation of capital charge for their operational risk as per Basel II instructions. Under these approaches, either gross income or a combination of gross income and outstanding advances is assumed to be the exposure indicator based on which operational risk capital charge is calculated. However, the corner stone of any operational risk management or capital allocation under advanced approaches of Basel II is the historical time series of operational loss data.

In terms of modern operational risk management, banks operating in Pakistan are at infancy stage and very recently some banks have started collection of loss data with a view to use the same in their operational risk assessment and capital allocation. Under the existing SBP instructions, banks only report cases pertaining to frauds, forgeries and dacoities on quarterly basis which provide limited information regarding operational losses within the banks. In order to enhance the scope of loss data gathering in line with the Basel II requirements and provide the industry with a minimum set of instructions for consistent recognition of losses and their reporting to a data consortium, SBP has formulated these guidelines. Following are the main objectives of this initiative:

- Implementation of effective operational risk management framework by adopting international best practices and inculcating risk awareness culture within banks.
- Start collection of operational loss data within banks/ DFIs on the Basel defined business lines/ event types matrix.
- Collection of industry wide loss data (from supervisory perspective the losses reported by banks) may be used for comparison and judging the operational riskiness of banks.
- Start gathering Key Risk Indicators (KRIs) and conduct Risk & Control Self Assessments (RCSAs) on an ongoing basis. The RCSA and KRI are modern techniques whereby an institution can keep an eye on existing as well as future dimensions of operational risk.
- The advanced method for calculating operational risk i.e. Advanced Measurement Approaches (AMA) is based on four elements i.e. internal data, external data, scenario analysis and business environment and internal control systems (BE&ICS). These guidelines would provide basis for collecting internal and external data and BE&ICS. All banks would consistently track operational risk losses and relevant data for effective management of operational risk and may form basis for the implementation of advanced approaches in the future.

The first section provides Introduction and objectives of operational risk. The second and third sections cover BCBS publication regarding the principles of sound operational risk management. These sections are intended to update SBP risk management guidelines of 2003 pertaining to operational risk.

The section four to eight provide the supervisory expectations regarding risk identification, assessment, reporting and monitoring. Banks under these guidelines would develop their internal database and going forward report their losses over certain threshold to the data consortium - a mandatory requirement to implement advanced approaches of operational risk under Basel II. Moreover, banks would be required to set up a system of reporting/ monitoring under which the material losses would be reported to higher management and to the Board of Directors.

Regarding Business Environment and Internal Control Systems, these guidelines require banks to instill a system for gathering Key Risk Indicators and conduct Risk & Control Self Assessments on an ongoing basis so that the banks apart from knowing what has gone wrong in the past can keep an eye on the probable key risks and control breaches that may cause future losses.

Under these instructions, banks are instructed to collect/ gather key risk indicators along with actual loss data and on best efforts basis reconcile it with general ledger, on quarterly basis.

*****

1. Introduction & Objectives

1.1. SBP has been encouraging banks to follow international best practices and instill sound risk management and corporate governance culture. In this regard, SBP has been issuing instructions from time to time which include the following main circulars:

i. Risk Management guidelines were issued vide BSD circular 7 of August 15, 2003 to provide broad level guidance on various risks (including operational risk) faced by the banks.
ii. Guidelines on Internal Controls were issued vide BSD Circular 7 of May 27, 2004, to ensure existence of an effective internal control systems.
iii. Business Continuity Planning guidelines were issued vide BSD circular 13 of September 4, 2004, in which the banks were advised to develop effective contingency and security plan.
iv. SBP Implementation of Basel II guidelines issued vide BSD circular 8 of June 27, 2006 which in addition to credit and market risks also require banks to allocate capital for operational risk based on prescribed approaches.

1.2. Operational risk has been defined as the risk of loss resulting from inadequate or failed internal processes, people and system or from external events. It includes legal risk but exclude strategic and reputational risk[1]. The definition attempts to categorize underlying causes of operational risk in a much broader prospective i.e. people, processes, systems and external factors. However, the scope of operational risk does not include following events (and resultant losses) as these are to be covered under Pillar 2 of Basel II accord.

i. Strategic Risk - senior management's business decisions in normal course of business which do not violate any rule, regulation etc.
ii. Reputational risk – as it arises mainly due to occurrence of other risk events.

1.3. It is imperative that banks try to prevent frauds and reduce transaction errors by maintaining strong emphasis on internal controls and develop their human resources. With ever changing business environment, product complexity, diversification, increased quantum of electronic transactions and outsourcing; banks are required to set up a mechanism for ongoing evaluation of their true operational riskiness according to their size, sophistication, nature of operations and expected level of capital.

1.4. Operational risk is an evolving discipline and hence significant flexibility is available to banks in developing operational risk measurement and management systems. Some of the banks have already initiated collection of their operational risk loss data with a view to use the same for the assessment of inherent and residual risks with possible extension towards measurement of risk based performance and allocation of capital. Hence, to provide industry a minimum set of instructions for meeting the supervisory expectation under Basel II requirements and to address some of the key challenges faced by the banks when collecting internal operational losses, SBP has formulated these guidelines with the goal of promoting consistency, completeness and accuracy in the collection of operational risk data which would form the basis for risk analysis and control to be used

[1] *Definition adopted from International Convergence of Capital Measurement & Capital Standards – A revised framework comprehensive version, June 2006*

for effective operational risk management and for moving towards advanced approaches for calculation of operational risk capital charge.

2. Principles for Sound Management of Operational Risk

Operational risk is inherent in the banks activities and is an important element of enterprise wide risk management system. In the past few years, significant progress has been made in the area of implementing operational risk management framework and accordingly following main principles[2] for the sound management of operational risk have emerged. All banks are advised to follow these principles in their approach to operational risk management.

2.1. The ultimate responsibility and accountability rests with the board of directors to ensure that a strong risk management culture exists throughout the organization. The board can delegate this responsibility to senior management with clear guidance and direction to inculcate a risk culture within the organization.

2.2. The bank should develop, implement and maintain Operational Risk Management Framework which should be integrated into bank's overall risk management processes. The framework should be documented, duly approved by the board and at the minimum should:

i. Define the terms "operational risk" and "operational loss".
ii. Identify governance structure, reporting lines, responsibilities and accountabilities.
iii. Describe various risk assessment tools and modus operandi on the effective use of these tools.
iv. Describe the bank's accepted operational risk appetite and tolerance levels, and thresholds limits for inherent and residual risks with approved risk mitigation/ transfer strategies.
v. Define bank's approach for establishing and monitoring thresholds/ exposure limits for inherent and residual risk exposure.
vi. Describe risk reporting mechanism and appropriate hierarchy level at which the reporting would be escalated.
vii. Provide common definition/ classification terminology to ensure consistency of risk identification, exposure ratings and risk management objectives.
viii. Describe process of independent review and assessment of operational risk by Audit or independent qualified personnel.
ix. Define process of updating the framework on an ongoing basis and whenever a material change in the operational risk profile of the bank occurs.

2.3. The board of directors should establish, approve and periodically review the Framework and should oversee senior management to ensure that the policies, processes and systems are implemented effectively at all decision levels. The framework should be reinforced through a strong internal control environment with clear lines of management's responsibility and accountability. The control environment should provide appropriate

[2] Basel Committee on Banking Supervision paper on "*Principles for the Sound Management of Operational Risk and the Role of Supervision" – June 2011,* which can be accessed through website http://www.bis.org/publ/bcbs195.pdf.

independence/ separation of duties between operational risk management function, business lines and support functions.

2.4. The Board is responsible to approve and review risk appetite[3] and tolerance statement for operational risk depending on nature, size, and complexity of business, current financial condition and the bank's strategic direction. The risk appetite and tolerance statement should capture the past and future aspects as part of their risk management and capital assessments. The banks may express risk appetite in shape of loss data thresholds, Risk Control Self Assessment remedial action prompts and Key Risk Indicators thresholds. Moreover, with change of business and control environment, the board should regularly review the appropriateness of threshold or limits for specific operational risks and an overall operational risk appetite and tolerance.

2.5. Senior Management is responsible to develop governance structure with transparent, well defined and consistent lines of responsibilities. The governance structure after approval from the board would be implemented and senior management should ensure that policies, procedures and systems to manage operational risk cover all material products, activities and processes in line with the established risk appetite and tolerance. The role of management is to effectively communicate laid down procedures / guidelines down the line and across various business lines to put in place a reasonable system for implementation of policy.

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

2.7. It is the responsibility of management that before the introduction/ launch of new products, activities, processes and systems; there must be an approval system to adequately assess operational risk inherent in these initiatives. The approval process at the minimum should ensure that the product/ activity added is in line with the risk appetite/ tolerance level and adequate human, infrastructure and necessary controls are available to carry out introduced activities.

2.8. For proactive management, senior management should implement a process to regularly monitor operational risk profiles and material exposures to losses. The ongoing monitoring necessitates the establishment of an effective and efficient reporting mechanism to the board, senior management and business lines. The reporting at the minimum should contain breaches of tolerance limits, details of significant internal or external operational risk events that can affect bank's operational risk profile.

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

[3] *The term 'risk appetite' is often used for forward-looking view of risk acceptance while 'risk tolerance' is often taken as the amount of risk a bank has accepted in the past.*

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

2.11. For transparency and market discipline, banks are advised to properly disclose their approach of operational risk management to its stakeholders.

3. Management of Operational Risk

3.1. Risk management generally encompasses the process of identifying risks, measuring exposures to those risks, ensuring that an effective capital planning and ongoing monitoring program is in place, taking steps to control or mitigate risk exposures and reporting to senior management and the board regarding the bank's risk exposures and capital positions.

3.2. Internal controls are typically embedded in a bank's day-to-day business and are designed to ensure, to the extent possible, that bank activities are efficient and effective, information is reliable, timely and complete and the bank is compliant with applicable laws and regulation.

3.3. In practice, the terms "risk management and internal controls" are closely related and the distinction between both is less important than achieving the objectives of each. The objectives of managing operational risk at the minimum include reducing avoidable losses and insurance costs, improving awareness and transparency of risk and providing evidence regarding effectiveness of control procedures.

3.4. The board should set strategic direction for operational risk management within the organization. Banks should have in place an operational risk strategy aligned with the business strategy which needs to be continuously updated and must include framework implementation plan for next 3 years. There should be clear and unambiguous board and senior management support/ sponsorship for the success of operational risk management framework/ function and same level of emphasis/ priority must be given to operational risk as that of credit, market or liquidity risk.

3.5. The board (or its delegated committee) must have clear understanding of operational risk as a distinct risk category and be aware of the key risks faced by the institution. For this purpose, the bank should collect and report data which should be accurate, comprehensive and allows the bank to anticipate potential future problems. The collected data should be sufficiently granular to support detailed analysis by risk factors. The data reporting from origination to the board should accompany value adding analysis and summaries consistent with the decision making status of the recipients.

3.6. The operational risk management by definition involves managing human error and inadequacies; however there is a tendency of employees/ line management to hide errors. In order to overcome this tendency the board and senior management should work on enhancing risk awareness and establishing a risk culture within the

organization. The effectiveness of bank's operational risk governance and risk management structure would be evaluated by SBP based on the quality of implementation and its impact on awareness of staff regarding their responsibility to identify, manage, monitor and report operational risk. Moreover, the remuneration policies should also be consistent with the approved risk appetite. Managers should not be rewarded solely on the basis of profits, but audit findings and compliance status should also be considered while deciding bonuses and compensations.

3.7. For effective management of operational risk, each bank should establish an independent operational risk management function. Banks need to ensure that the function has adequate and qualified human resource with technical capacities to manage operational risk. Operational Risk Management function should be designated with the following responsibilities;

i. Developing and updating operational risk policy and ensuring that operational risk management is carried out as per approved policy.
ii. Developing and maintaining operational risk framework to improve the way in which operational risk is identified, assessed, controlled, mitigated, reported and monitored.
iii. Communicate and coordinate with various risk management activities/ business lines and suggest plans for minimizing risk and improving the internal controls.
iv. Providing independent opinion to senior management and the board regarding products/ activities that can significant alter operational risk profile of the bank.
v. Set up a system for consistent and comprehensive operational risk data gathering and to present their findings to the business line managers, senior management & the board for review of bank's progress towards stated policies/ objectives.

3.8. For the sound operational risk governance, the bank should rely on following three lines of defense. It is vital that these lines of defense have a common goal of promoting risk culture within the organization with open channels.

i. The prime responsibility of operational risk management rests on business line management which is responsible for identifying and managing risks in the products, activities, processes and systems for which they are accountable. It is important that clearly documented and regularly updated operating manuals are readily available to all the employees. Segregation of duties needs to be ensured and operational staff must have necessary skills and training so that they can fulfill their duties.
ii. A separate function independent of internal audit should be established for effective management of operational risks in the bank. Generally, such a function is established under the risk management department/ division. Independent operational risk management function would assist management to understand and manage operational risk. The function is responsible to assist in establishing policies and standards and coordinate with various businesses/ risk management activities. The function would assess, monitor and report operational risks as a whole and ensure that the management of operational risk in the bank is as per

approved strategy/ policies. The independent operational risk management unit/division should be capable of challenging business lines input/ output towards bank's risk management, measurement and reporting systems.

iii. Independent validation and verification is the third line of defense in the governance structure used to manage operational risk and it serves as a challenge function to the other two lines of defense. Internal audit or any independent group of qualified staff may conduct these independent reviews on the effectiveness of operational risk management function and operational risk measurement system (ORMS). The below section provides some of the supervisory guidelines associated with the verification and validation and role of audit function.

Verification & Validation

3.9. The operational risk measurement system (ORMS) is a subset of an operational risk management framework. The ORMS consists of the systems and data used to measure operational risk in order to estimate the operational risk capital charge. The ORMS must be closely integrated into the day-to-day risk management processes.

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

3.11. The validation activities conducted by internal audit provide opinion whether the capital held (or estimated) is fulfilling internal and supervisory purposes. The validation activities are mostly designed to provide opinion regarding the operational risk model working. However, at this stage bank's validation activities should ensure that ORMS used by the bank is robust and provide assurance regarding integrity of input, process, assumptions (if any) and output. The work of internal validation also covers qualitative aspects such as validation of data inputs, reporting, role of senior management and methodology/ intended use of operational risk models etc.

3.12. The periodic verification activities can be conducted by the bank's internal and/or external audit or other independent parties. The verification ensures the following:

i. Policies, processes, procedures and systems which comprises the bank's operational risk management framework including ORMS is conceptually sound, transparent and documented.
ii. Business unit activities, the independent operational risk management function and governance committees and structures are effective and appropriate.
iii. The framework input and outputs are accurate, complete, credible, relevant, authorized and accessible.
iv. Risk monitoring and management of the accuracy and soundness of all significant processes and systems are effective.

v. Appropriate remedial measures are undertaken whenever deficiencies are identified.
vi. Comparisons of RCSA, KRIs and scenario results with the actual loss experience (internal data or external data) are done effectively.
vii. Tests of controls determine whether these controls are designed to prevent or detect and correct material deviations/ non-compliance with the policies/ procedures and operate effectively throughout the period being reviewed.
viii. Every significant activity of the bank, as well as subsidiaries of the bank, must be included.

3.13. Results from verification and validation work should be documented and distributed to appropriate business lines management, internal audit, operational risk management function and appropriate risk committees. Bank staff ultimately responsible for the validated unit should also have an access and understanding of these results.

3.14. Reporting of verification and validation work should also include underlying processes to resolve deficiencies and weaknesses, ensuring that corrective actions are implemented in a timely manner. Internal audit should also evaluate management's response to significant findings.

3.15. Results of verification and validation reviews should be summarized and reported annually to the bank's board of directors and committee thereof. Confirmation by senior management entails review and approval of the effectiveness of the bank's operational risk management framework including operational risk management system.

3.16. The verification and validation reporting should:
i. Summarize the verification and validation work done; indicate any limitations in the scope of work performed and details of deviations from the plan, if any.
ii. Identify weakness and their potential consequences, including deviation from policy, procedures and Basel (II & onward) requirements.
iii. Establish a corrective action plan and specific timeline for remediation for significant deficiencies and weaknesses.

Control Effectiveness

3.17. The bank should have adequate processes in place to monitor the identified controls and ensure they are appropriate to mitigate the identified risk to the desired residual level. The processes should include the identification, review, escalation and remediation of the issues identified.

3.18. With the ever increasing role of IT in the banking sector, the banks should conduct periodical reviews of access rights to the core banking and other sensitive systems. Banks should establish procedures that only qualified and relevant personnel have the password (access rights) to the sensitive IT systems including core banking. The bank may review the list of authorized persons periodically depending on the sensitivity of the system/ transactions.

4. Risk Identification & Assessment

4.1. The key elements in the operational risk management framework are:

i. Risk identification and assessment
ii. Risk monitoring and reporting
iii. Risk control and mitigation.

4.2. Risk identification is vital for the development of a robust operational risk monitoring and control system. Effective risk identification should consider both internal and external factors which could adversely affect the achievement of the bank's objectives.

4.3. Operational risk is inherent in all the business activities and processes of banks; hence banks should identify and assess operational risk inherent in all material products, processes, activities etc. The business units have the best knowledge of their risks and processes hence these units should play a major role in risk identification. The bank should document reasons if any activity is left out from risk identification/ assessment process.

4.4. For minimizing operational loss events, identification of risk and proper recording is inevitable. Data requirement for operational risk is complex and involve several dimensions.

4.5. Risk identification process aims to collect all relevant information which can be used in operational risk management process. The tools that are used to identify and assess operational risk include: internal loss data collection and analysis, external data collection and analysis, risk control self assessment, business process mapping, key risk indicators, scenario analysis, comparative analysis and audit findings.

4.6. The following are the recommended techniques/ tools for operational risk identification and assessment, however banks may use any other technique, if they can demonstrate to SBP that the basis requirements stated in this guidelines for robust risk identification and assessment are met:

i) Gathering of Internal Loss Data
ii) Risk Control & Self Assessment (RCSA)
iii) Key Risk Indicators (KRIs)

5. Internal Loss Data

General Requirements

5.1. The collection and analysis of bank's own loss data can provide vital information to management and provide basis for operational risk management and mitigation. However, most of the banks do not have documented history of operational losses. Therefore as a first step, banks need to set up a system for consistent and comprehensive loss data gathering.

5.2. Bank's internal loss data would mostly comprise of high frequency and low severity events with very few large losses. Such a database may not be relevant for quantitative modeling. However by studying trends of internal losses, banks can improve the efficiencies of its processes and internal controls. Hence, banks need to assess the depth of their data collection which may be used for risk management and/or risk quantification model.

5.3. The industry practices regarding risk modeling are in evolving stage, therefore the data collection system should have the inbuilt flexibility to adapt to such changes.

5.4. The scope of operational risk management includes internal inadequacies, events triggered by external causes and legal settlements. Banks should collect data for all losses pertaining to operational errors and internal control failures etc., even if such losses are related to the credit or market risk areas. However, banks should be able to tag their losses pertaining to market and credit risk by introducing a separate field in the database from rest of the losses. This would facilitate banks in the implementation of advanced approaches where these data points would be used separately for the modeling purposes.

5.5. The challenges banks are likely to face in building internal loss database would depend on the processes of collection, level of automation and nature of losses. Event data capturing system should be part of workflow and entire organization is expected to participate in operational risk event collection & reporting.

5.6. Another likely challenge for banks in loss data collection would be to get the involvement of employees. Banks will have to work on enhancing risk awareness and establishing a risk culture to avoid incomplete or erroneous data reporting. The bank should have policies regarding consistent recognition of operational losses and their reporting to internal loss data base. Further, to the extent possible, banks may verify number of losses and amount with their General Ledger.

5.7. Banks internal loss data must be comprehensive enough to capture material losses by business lines. The banks should have clear and consistent definitions for the collection of operational risk losses and documented criteria by which losses are allocated to specific business lines and event types. The adopted classification criteria should also contain methodology for classifying any new activity or product to be introduced in the future, into one of these business lines.

5.8. Banks/ DFIs are required to set up approval procedure/ policy for identification, collection and recording of losses in the centralized database. These procedures may provide guidance to any staff unfamiliar with the data collection processes. The policy should clarify the roles and responsibilities of operational risk management function and business line management regarding ongoing data management.

5.9. To ensure consistency and accuracy of data collection, the input in the database should be checked and approved by some approving/ counterchecking authority. Moreover,

depending upon the nature and severity of loss, bank should also establish a reporting mechanism to escalate the loss reporting to relevant designated authority.

5.10. A bank is responsible for defining and justifying appropriate thresholds for each operational risk class (e.g. business line (BL), event type (ET), combination of BL & ET, products etc.). Thresholds need to be defined for data capturing and loss reporting so that management has the ability to evaluate and react to operational risk events. The thresholds would depend on size of the organization and business line. Losses below certain threshold (amount) may not be captured by the banks because of cost involved. However, defining a threshold should not result in considerable loss of data, therefore, it is recommended that (for internal operational risk management) initially all losses above PKR 200,000 are captured and thresholds may be defined later on when sufficient data points are available, however in no case the threshold would exceed PKR 200,000. SBP expects banks to demonstrate that thresholds set are reasonable and does not have a material impact on the overall risk estimates (capital charge requirements).

5.11. Data collection thresholds should capture all material losses in terms of their value. However, determination of a threshold should be based on some research. Therefore a bank needs to verify, on a periodic basis that its choice of threshold includes all material operational risk losses for risk management purposes. For example, a bank may attempt to collect all below threshold items for a given period and then reconcile them with accounting data to examine the effect of including these losses in management action/ capital modeling.

Operational Risk Loss Reporting to Data Consortium

(Which may be hosted by SBP or any third party like PBA)

5.12. For reporting to centralize depository, an operational risk loss can arise only from an actual operational risk event which has a quantifiable negative impact on the profit and loss (P&L) statement of the bank.

5.13. The negative impact on P&L would be termed as Gross Loss i.e. loss before recoveries of any type. Whereas recovery is an independent occurrence, related to the original loss event, separate in time, in which inflows of economic benefits are received from the party concerned or from any third party. For an operational risk event, a bank should be able to discretely identify the gross loss amount as well as any recoveries there against including insurance recoveries.

5.14. Banks in future will report all events to data consortium where Gross Loss is greater than or equal to PKR 500,000. However, events of fraud, forgeries and dacoities (included attempted events) should be reported irrespective of the amount involved. Going forward, SBP may review thresholds level for data pooling and industry comparison when sufficient data is available at industry level.

5.15. Following items are included in the gross loss computation:

a. Direct charge (including impairments, write-downs) due to operational risk events and provisions/ reserves reflected in P&L statement for potential operational loss impact.
b. Costs incurred as a consequence of the event that should include external expenses with a direct link to the operational risk event (e.g. legal expenses directly related to the event and fees paid to attorneys) and costs of repair or replacement, to restore the position that was prevailing before the operational risk event.
c. Pending losses stemming from operational risk events with a definitive financial impact, which are temporarily booked in suspense accounts and are not yet reflected in the statement of P&L.

On the other hand, the following items are excluded from the Gross Loss computation:

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

5.16. All operational risk losses (number and amount) that have negative impact on profit and loss statement of the bank and are quantifiable would be reported to the centralized database in soft form on quarterly basis. Banks would separately submit summary sheets (hard copies) of losses to SBP (pertaining to current quarter as well as cumulative losses at each reporting date) as per **Annexure-A** & **Annexure-B**.

5.17. **Annexure-C** prescribes the minimum data fields for building loss database. Banks are, however, encouraged to select/incorporate additional data fields depending upon the target regulatory approach for calculating operational risk capital charge. Banks are further required to record some descriptive information about the drivers or causes of the loss event. However, for internal management, the bank may use loss data base as the depository for investigation and casual analysis which may also influence the choice of data fields in depository.

5.18. Banks are free to adopt any definition/ methodology for internal operational risk management and data collection, however, for quarterly reporting to data consortium, the banks shall maintain standardization of loss data i.e. losses must be systematically tracked by eight business lines (up to Level 2) and seven event types (up to Level 3) as specified under SBP Basel II guidelines for the standardized approaches of operational risk.

5.19. Banks may only add event type at level 3, after notifying data consortium, subject to the condition that loss event could not be mapped with Basel defined activity examples (level 3) and there are significant instances so that defining activity at level 3 may add value to operational risk management.

5.20. The banks are required to follow BCBS guidelines for consistency and standardization of mapping losses among various Event types/ Business lines. However, in case the BCBS instructions do not provide adequate guidance then banks may opt for the best market practices in this regard by notifying SBP. One of the methodologies being recommended is proposed by Samad Khan (2002)[4] which is based on a payoff matrix whereby losses are allocated according to (i) who benefits or intended to benefit; (ii) who loses or intended to have lost directly or economically.

5.21. Business Lines represent profit centers from where the bank makes profit/ commission. However, there is a possibility that some events may affect the cost centers (i.e. some centralized group services, such as Human Resources, IT etc.). In order to create harmonization for centralized loss depository, such centralized losses may be reported as a separate business line "Cost Centers". The code list is appended as **Annexure-E**. This is an exception from SBP Basel II guidelines which prescribe that these ancillary functions must be allocated to the business line it supports and if more than one business line is supported through the ancillary activity, an objective mapping criteria must be used.

5.22. The date of loss event may have significant impact on the assessment of bank's operational risk profile. It is possible that some losses may not be detected until months after the loss event has occurred. For reporting to data consortium, three dates (occurrence, discovery and date of financial impact) are to be submitted with each event record.

5.23. In case the bank compensates a client for an operational risk event through reduced charges, such lower charges which affects the revenues are to be reported as Gross Loss.

5.24. In case of damage/ total destruction of fixed assets, the banks should report the Market Value of the assets prior to the incident as Gross Loss in case the asset is not replaced. However, in case of replacement, the bank should report cost of replacement as Gross Loss. The replacement cost means the cost to replace an item or to restore it to its pre-loss condition.

5.25. The loss in Investments and Intangible Assets due to operational risk event is to be reported as per the Economic Value or cost of replacement.

5.26. All regulatory penalties and fines over the defined threshold are to be reported. The fines pertaining to a single cause may be grouped as described in next paragraph.

5.27. Multiple associated losses resulting from the same underlying cause may be grouped and can be treated as a single loss (one event) for recording and management. However, banks are expected to have internal loss data policy which may provide guidance for

[4] *Samad-Khan (2002), How to Categorize Operational Losses? – Applying Principles as Opposed to Rules, OpRisk Analytics, LLC. The document is available through website: http://www.opriskadvisory.com/docs/ORA_on_Categorization_-_A_Solution.pdf*

deciding the circumstances, types of data and methodology for grouping data. A bank may document judgments of its individual in applying these policies. For these grouped losses, the bank should report to depository the date of last discovered/ accounted loss (occurrence, discovery, date of financial impact) even if multiple losses are posted at different time in the General Ledger.

5.28. It is possible that a single loss event may affect multiple business lines. For reporting purposes to centralize depository, the amount should be assigned to each business line affected. The approving/checking authority should ensure that total loss remains the same and double reporting of losses should be avoided. However, for internal purposes, banks may also develop criteria for assigning loss data from an event in an activity that spans more than one business line.

5.29. There can be a time lag between a legal case initiation and its settlement/ decision. The banks should report all lawsuits (whether as plaintiff or defendant) and out of court settlements pertaining to operational risk loss when they negatively impact P&L. The gross loss may include external lawyer's fee, settlement cost and other litigation related expenses. For reporting to depository, litigation related losses should be reported based on conservative approach i.e. such cases should be reported when a bank establishes a legal reserve based on bank's provisioning/ accounting practices. Since a legal exposure can change over time, the bank should keep assessing its potential impact and update legal event exposure prior to the date of settlement. However for internal management purposes banks can populate internal database with potential or expected losses on discovery/ receiving of legal notices.

5.30. Timing losses are due to operational risk events which impact the cash flow or financial statements of previous accounting periods. Timing impacts typically relate to the occurrence of operational risk events that result in the temporary distortion of an institution's financial accounts (e.g. revenue overstatement, accounting errors and mark-to-market errors). Such losses are to be excluded from the reporting requirement subject to the condition that they are not "material". The material timing losses (greater than 5% of profit before tax) due to operational risk events that span two or more accounting periods should be included.

5.31. Rapidly recovered loss events are operational risk events that lead to losses recognized in financial statement that are recovered over a short period e.g. within 5 working days from the date of recognition. When recovery is made rapidly, the bank should report the entire loss as gross loss and any recovery pertaining to this loss may be shown as part of recoveries.

5.32. For calculating monetary impact of business disruptions or system failures (e.g. utility outage), the banks may split costs into two parts (i) direct cost – cost of employee time lost and cost of critical tasks which needs to be performed elsewhere (ii) opportunity cost – estimated amount of revenue that could have been generated during the down time. The unbudgeted costs pertaining to staff, loss data and remediation/ process improvement needs to be reported.

5.33. Items, such as Near Miss events, operational risk Gain Events and Opportunity Cost (lost revenue) are NOT required to be reported to the loss data consortium.

Recommended Practices (Optional)

5.34. Apart from capturing monetary losses, non-monetary losses (loss of profit, opportunity costs etc), control breaches and near-misses should also be recorded by the banks for their own risk management. All such cases where the bank recovers the entire amount involved and does not suffer any loss may also be captured.

5.35. Near misses can play a useful part in conducting scenario analysis which adds future-looking dimension to loss data. Near misses are also important for highlighting weaknesses and can help to determine whether the loss was avoided because of experience, luck or controls.

5.36. Banks may also develop documented procedures for assessing the ongoing relevance of historical loss data. For comparison purposes bank may use judgment overrides, scaling or other adjustments. For example, inflationary impacts and scale adjustments for meaningful comparison with previous year's losses.

6. Risk Control & Self Assessment (RCSA)

6.1. Apart from internal loss database, banks are encouraged to use other risk identification/ monitoring tools like Risk Control & Self Assessment (RCSA) and Key Risk Indicators (KRIs). These tools not only add a future dimension but also assist to capture cause-effect relationship of risks. Together with loss data, RCSA and KRIs provide a bank better understanding of its business environment and internal controls.

6.2. RCSA is the process in which potential material risks are indentified and recorded along with their related controls. The exercise primarily aims to support the bank in assessing adequacy of bank's risk management and effectiveness of its control processes. RCSA increase the awareness/ transparency of risk and help banks to evaluate the level of risks against pre-determined risk appetite/ tolerance levels.

6.3. Apart from helping the management to identify and assess the current level of operational risks and related controls, the exercise should also focus on identifying and assessing future potential risks since most of the biggest operational risk losses arise from some new issues which are difficult to forecast. Accordingly, the scope of RCSA may be enhanced by using Scenario Analysis (plausible but extreme potential future events) which would address the completeness of operational risk exposure and test the controls installed.

6.4. RCSA is a three tier process (as explained under point 6.6) where evaluation of risks and controls is done by the staff that actually performs the activities. These self assessments

encourage employees to assume responsibilities & accountabilities by improving their understanding regarding effective control and risk management. The improved understanding goes a long way in assisting an organization to effectively implement any corrective actions.

6.5. RCSAs can be done through process mapping, brain storming session, surveys, workshops and expert judgment/ interviews. There is no best approach to carry out self assessment exercises; hence a bank, depending on its circumstances and availability of resources should select the appropriate approach. However, it is also a recommended strategy that the same facilitator or group of participants may not be used repeatedly as it can result in stereotype conclusions. An illustrative template of RCSA is provided at **Annexure-D.**

6.6. The banks may select a process-based approach for self assessment under which each process (sub-process) from beginning to end is documented. Under the first step of the three tier process of self assessment, banks may describe the risks inherent in each process and its impact assuming that there are no controls. In the second phase, bank would be able to describe the controls employed to cover these identified risks and to identify key controls in the underlying process. The third information pertains to residual risk assessment (inherent risk after considering controls). The banks are expected to identify/ assess control weaknesses and other specific risks associated with each process under review.

6.7. The identified risks may be assessed based on the judgmental scoring or thresholds (probability of risk materializing, monetary impact etc.). The assessment may be done either at inherent or at residual level by considering both risk probability and severity. Adopting risk assessment both at inherent and residual level provides more insights into the nature of the risks and controls. However, since the banks are in their initial stage of implementing these concepts, therefore SBP is currently prescribing risk assessment on residual basis; going forward it is expected that banks will also conduct inherent risk assessments. For the purpose of scoring, the bank may develop any scales ranging from low (low probability, low severity) to high (high probability, high severity)[5]. The risk assessment process may further include assessment of controls (risk mitigation) to assess the effectiveness of controls by considering existing controls measures and potential events (internal and external). Furthermore, in case the residual risk is excessive (compared to target residual risk) an action plan should be devised with clear deliverables and target dates.

6.8. The RCSA exercise can result in accumulation of a large volume of information. However, the operational risk management function of the bank is responsible for reporting results (i.e. identified risks and control weaknesses) and corrective action plan to the senior management in a meaningful manner.

[5] *For example, the scores ranging from 1 to 5 may be assigned each to probability and severity where 5 represent High. The overall risk score is then calculated by multiplying probability by severity and resultantly overall risk score between 1 to 25 may be calculated.*

6.9. Self assessment exercise oriented towards key risks and controls should be an ongoing/ regular activity. Ideally, banks should review its RCSA on annual basis (or whenever there is a breach of control) in view of the improvements or deterioration in business and controls. These periodic exercises are aimed to provide the bank with a better understanding of its risk profile.

6.10. The RCSA sessions/workshops can help inculcate culture of openness and transparency. The self assessments are expected to generate discussions to improve awareness, sharing of knowledge and allocation of resources.

6.11. Banks should establish a routine where actual losses are compared with the results of assessment exercises.

7. Key Risk Indicators (KRIs)

7.1. Key Risk Indicators (KRIs), are measurable indicators which can be termed as early warning signals, provide information regarding increased current or potential level of operational risk exposure to help institution measure and manage emerging risks by identifying risk symptoms. The indicators ensure that the risk monitoring is focused on the key risks to which an institution is exposed.

7.2. KRIs selection process starts by analyzing the already identified key risks as a result of RCSA exercises, audit reports, industry environment and actual loss experiences. The analysis of past events helps in the identification and finding of the intermediate event or root cause event which led to the loss. Moreover, banks need to have firm understanding of their organizational objectives and need to identify future risk events (based on scenario analysis) that may affect the achievement of those objectives.

7.3. The goal of an effective KRI is to pin point the ultimate root cause of the risk event. The indicator is designed to transmit meaningful and timely information to the management enabling them to take corrective actions to evade potential operational losses before they happen or become larger. Hence, effective indicators are closer to the root cause of event and provide more time to management for proactive action[6].

7.4. A single indicator may or may not adequately capture the trends of a key risk. Therefore, the banks may analyze a collection of KRIs simultaneously for better understanding of the risk being monitored.

7.5. The selected KRIs should contain the following characteristics;

i. Be effective in tracking an important risk.

[6] *Developing Key Risk Indicators to Strengthen Enterprise Risk Management, Research commissioned by COSO, December 2010*

ii. Must have the predictive power to prevent a future loss i.e. leading KRIs are more desired.
iii. Be practical and easy to collect i.e. measurable and quantifiable.
iv. Track at least one aspect of risk profile i.e. risk cause, event, effect and control.
v. Can serve as a mean to express risk appetite.

7.6. KRIs can be specific and generic. Specific indicators relate to one or very few business units while generic indicators are collected by many business units.

7.7. For collection of KRIs, the bank should establish;
i. Clear responsibilities defining persons to whom these indicators are assigned.
ii. Standardized definitions for understanding of entire staff across the organization.

7.8. Key Risk Indicator alerts management if they go outside the established range. Therefore banks may define acceptable ranges and in case of breach of threshold, actions to be taken by managers to accept or mitigate the risk are to be recorded. Due to lack of historical data, the setting of thresholds at initial stages is not possible; however, after one year of implementation, the banks are expected to have enough data to define thresholds.

7.9. Identification of KRIs is also not a onetime exercise as KRIs will change over time as organizational risks and strategies change. Processes need to be established to reassess the value of identified KRIs and to determine the need for new indicators. Bank should set up KRI validation cycle on yearly basis in which thresholds may also be reviewed/ revisited.

7.10. Apart from bottom up method of identifying KRIs, top down approach can also be used whereby top management, keeping in view the internal and external factors, identifies risk faced by the entity.

7.11. Banks shall identify and monitor at least 15 risk indicators in each business line on an ongoing basis. Senior management and the board of directors are expected to understand and remain updated on most significant KRIs pertaining to the institution's top 10 risks. Accordingly, banks should set thresholds for regular monitoring and reporting. At this stage, reporting of KRIs to data depository is not being prescribed; however, SBP would review bank's progress in this regard.

8. Reporting & Action Plans

8.1. The purpose of operational risk data tools (loss data, RCSA & KRIs) is to find key risk factors and drivers to develop understanding of the causes and consequences. The key drivers of operational risk are people, processes, system and external dependencies[7]. Based on findings of data, bank should be able to take appropriate corrective actions.

[7] *The Operational Risk Manager's Guide, Tools and Techniques of the Trade, Sergio Scandizzo, 2007*

8.2. Banks internal reporting policies should include clearly defined escalation policy whereby losses over certain thresholds, significant event, critical (present or potential) risk and control breaches are immediately reported to senior management as per defined criteria. There should be regular and timely reporting of losses to various level of management and to the board of directors.

8.3. Regarding the ongoing monitoring, banks should have procedures for taking appropriate actions on losses being reported. Banks should record high level comments on significant losses and action taken by respective level of management. These action plans once decided must be documented and reviewed. The progress in this regard should also be included in ongoing reporting.

8.4. All banks/ DFIs are expected to set up operational risk data collection mechanism by December 2015. Moreover, it is expected that within next three years when sufficient loss data point are available, the bank should be able to conduct an empirical analysis as to how their operational risk varies with the expansion/ contraction of their operations/ business cycles.

******

References

- *International Convergence of Capital Measurement and Capital Standards: A Revised Framework – Comprehensive Version, BCBS, June 2006*
- *Principles for the Sound Management of Operational Risk, BCBS, June 2011*
- *Supervisory Guidelines for the Advanced Measurement Approaches, BCBS, June 2011*
- *Information Paper, the Utilization of Internal Loss Data in the Measurement and Management of Operational Risk in Australian AMA Banks, APRA, July 2008*
- *Operational Risk Reporting Standards (ORRS), Edition 2011, ORX Association*
- *Developing Key Risk Indicators to Strengthen Enterprise Risk Management, Research commissioned by COSO, December 2010*
- *How to Categorize Operational Losses? – Applying Principles as Opposed to Rules, OpRisk Analytics, LLC, Samad Khan, 2002*
- *A Short Guide to Operational Risk, David Tattam, 2011*
- *The Operational Risk Manager's Guide, Tools and Techniques of the Trade, Sergio Scandizzo, 2007*

Annexure-A: Quarterly Summary Data Reporting

Business Lines	Event Type Category (Level 1)											Total Losses by Business Lines			Gross Income (as defined in SBP Basel instructions on Operational Risk)	Gross Losses as % of Gross Income	Net Losses as % of Gross Income
	Internal Fraud					External Fraud				Employment Practices & Workplace Safety	Clients, Products & Business Practices	Damages to Physical Assets	Business Disruption, System Failure	Execution, Delivery & Process Mgt.			
	No. of Events	Gross Loss	Net Loss	Threshold applied	Max. Single (Net) Loss					5 columns	5 columns	5 columns	5 columns	5 columns	No. of Events	Gross Loss	Net Loss
Corporate Finance (CF)																				
Trading & Sales (TS)																				
Retail Banking (RB)																				
Commercial Banking (CB)																				
Payment & Settlement (PS)																				
Agency Services & Custody (AS)																				
Asset Management (AM)																				
Retail Brokerage (RBK)																				
Cost Centers (COST)																				

{Separate statements for current quarter losses and cumulative losses (year till date) are to be submitted}

Annexure-B: Major Operational Risk Losses (PKR 5 Million & above) – Which are still open or which are recorded in Last one Year

Loss ID #	Gross Loss (Amount (in PKR)	Un-recovered Amount	Status (Open/ Closed)	Recovered Amount			Breakdown of Gross Loss (%) by Business Lines									Risk Event Type	Event Dates			
				Directly	From Insurance/ other risk transfer methods	Estimated recovery in future	CF	TS	RB	CB	PS	AS	AM	RBK	COST		Incident	Detection	Accounting	Latest recovery date

Annexure-C: Internal Loss Data Fields

General Information				Incident Information								
Loss ID #	Reporting Unit (Branch/ Office)	Geographic Location	Reporting Person	Description of Loss incident	Individual Involved	Cause of the incident (New risk, control failure, other)	Cause Categorization (People, processes, systems or external events)	Mitigation/ Remedial Actions (Action due date & Action completed or not?)	Status (Open/ Closed) Date of closing (if closed)	Discovered by & How	Business Line (Basel Defined) a) Level 1 b) Level 2	Event Type a) Category 1 b) Category 2 c) Category 3
1	2	3	4	5	6	7	8	9	10	11	12	13

Incident Information							
Incident Date	Detection Date	Accounting Date	Related to Credit Risk (CR) or Market Risk (MR)	Gross Loss (in PKR)	Mention Currency (if different from PKR)	Recovered Amount a) Directly b) Insurance c) Other recovery	Latest Recovery Date
14	15	16	17	18	19	20	21

Additional Incident Information (not to be reported to data consortium)		
Expected Recovery	Potential Loss (in case of litigation cases)	Attempted Fraud/ Near Miss/ Control Breaches a) No. of attempts/ control breaches b) Frequency (High/ Medium/ Low) c) Severity (High/ Medium/ Low)
1	2	3

Annexure-D: Illustrative Template for Risk Control & Self Assessment & KRIs

RCSA information					
Business Line(Basel)	Functional/ Business unit	Unit Manager	RCSA approving Manager	Approving Date	Review Date

Process/ sub process	Basel II Event Type Category (Level 1)	Risk Description	Inherent Risk Assessment		Mitigating/ Control Description	Residual Risk Assessment			Process Owner	Control Owner	Key Risk (Yes/ No)	Key Control (Yes/ No)	Key Risk Indicator				
			Probability	Severity		Probability	Severity	Overall Risk Assessment					Description of KRI/ Control Indicator	Threshold	Current Status	No. of Loss incidents reported	Gross Loss Amount

Action Plan				
Type (KRI Threshold or Control Breach)	Description of deficiency	Required Corrective Action	Responsibility Staff Name	Target Date of Completion

Note: This template serves as an illustrative example only for the basic understanding and the fields contained therein may not be treated as completely exhaustive. Banks/ DFIs may customize this template keeping in view the complexity of their operations.

Annexure-E: Code List

Event Types

Event-Type Category (Level 1)	Definition	Categories (Level 2)	Activity Examples (Level 3)	Codes
Internal fraud (ET01)	Losses due to acts of a type intended to defraud, misappropriate property or circumvent regulations, the law or company policy, excluding diversity/discrimination events, which involves at least one internal party	Unauthorized Activity (ET0101)	Transactions not reported (intentional)	ET010101
			Transaction type unauthorized (w/monetary loss)	ET010102
			Mismarking of position (intentional)	ET010103
		Theft and Fraud (ET0102)	Fraud / credit fraud / worthless deposits	ET010201
			Theft / extortion / embezzlement / robbery /dacoity /attack on ATM / Locker breaking	ET010202
			Misappropriation of assets / Funds, Pocketing, Parallel banking	ET010203
			Malicious destruction of assets	ET010204
			Forgery (including mail spoofing & web spoofing)	ET010205
			Check kiting	ET010206
			Smuggling	ET010207
			Account take over / impersonation	ET010208
			Tax non-compliance / evasion (willful)	ET010209
			Insider trading (not on bank's account)	ET010210

			Falsification of accounts	ET010211
			Counterfeiting/card-skimming/trapping/PIN stealing	ET010212
			Forced Lifting of pledged stocks	ET010213
			Bribes/ kickbacks	ET010214
External fraud (ET02)	Losses due to acts of a type intended to defraud, misappropriate property or circumvent the law, by a third party	Theft and Fraud (ET0201)	Theft/Robbery/ dacoity /attack on ATM / locker breaking	ET020101
			Fraud / credit fraud / worthless deposits	ET020102
			Forgery(including mail spoofing & web spoofing)	ET020103
			Check kiting	ET020104
			Forced Lifting of pledged stocks	ET020105
			Account take over / impersonation	ET020106
		Systems Security (ET0202)	Hacking damage/attack on bank's server/media tapping/denying services	ET020201
			Theft of information/ Counterfeiting/card skimming/trapping/PIN stealing (w/monetary loss)	ET020202
Employment Practices and Workplace Safety (ET03)	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 (ET0301)	Compensation, benefit, termination issues,	ET030101
			Organized labor activities	ET030102
		Safe Environment (ET0302)	General liability (slip and fall etc.)	ET030201
			Employee health & safety rules events	ET030202
			Workers compensation	ET030203

		Diversity & Discrimination (ET0303)	All discrimination types	ET030301
Clients, Products & Business Practices (ET04)	Losses arising from an unintentional or negligent failure to meet a professional obligation to specific clients (including fiduciary and suitability requirements), or from the nature or design of a product	Suitability, Disclosure & Fiduciary (ET0401)	Fiduciary breaches/ guidelines violations	ET040101
			Suitability/ disclosure issues (KYC etc.)	ET040102
			Retails customer disclosure violations	ET040103
			Breach of privacy	ET040104
			Aggressive Sales	ET040105
			Account churning	ET040106
			Misuse of confidential information	ET040107
			Lender liability	ET040108
		Improper Business or Market Practices (ET0402)	Antitrust	ET040201
			Improper trade/ market practices	ET040202
			Market manipulation	ET040203
			Insider trading (on firm's account)	ET040204
			Unlicensed activity	ET040205
			Money laundering	ET040206
		Product Flaws (ET0403)	Product defects (unauthorized etc.),	ET040301
			Model errors	ET040302
		Selection, Sponsorship &	Failure to investigate client per guidelines	ET040401

		Exposure (ET0404)	Exceeding client exposure limits	ET040402
		Advisory Activities (ET0405)	Disputes over performance of advisory activities	ET040501
Damage to Physical Assets (ET05)	Losses arising from loss or damage to physical assets from natural disaster or other events.	Disaster and other events (ET0501)	Natural disaster losses	ET050101
			Human losses from external sources (terrorism, vandalism)	ET050102
Business disruption and system failures (ET06)	Losses arising from disruption of business or system failures	Systems (ET0601)	Hardware	ET060101
			Software	ET060102
			Telecommunications	ET060103
			Utility outage/ disruptions	ET060104
Execution, Delivery & Process Management (ET07)	Losses from failed transaction processing or process management, from relations with trade counterparties and vendors	Transaction capture, execution & Maintenance (ET0701)	Miscommunication	ET070101
			Data entry, maintenance or loading error	ET070102
			Missed deadline or responsibility	ET070103
			Model/ system misoperation	ET070104
			Accounting error/ entity attribution error	ET070105
			Other task misperformance	ET070106
			Delivery failure	ET070107
			Collateral management failure	ET070108
			Reference Data Maintenance	ET070109

		Monitoring and Reporting (ET0702)	Failed mandatory reporting obligation	ET070201
			Inaccurate external report (loss incurred)	ET070202
		Customer intake and documentation (ET0703)	Client permissions/ disclaimers missing	ET070301
			Legal documents missing/ incomplete	ET070302
		Customer/ client account management (ET0704)	Unapproved access given to account	ET070401
			Incorrect client records (loss incurred)	ET070402
			Negligent loss or damage of client assets	ET070403
		Trade counterparties (ET0705)	Non-client counterparty misperformance	ET070501
			Misc. non-client counterparty disputes	ET070502
		Vendors & Supplies (ET0706)	Outsourcing	ET070601
			Vendor disputes	ET070602

Business Lines / Area of operation

Business Line	Categories (Level 2)	Description	Codes
Corporate Finance (BL01)	Corporate Finance (BL0101)	Non-Municipal/Government Clients - Underwriting, Privatizations, Securitizations, Debt (Govt. & High Yield), Equity, Syndications, IPO, Private Placements, Mergers & Acquisitions, Research	BL0101
	Municipal /Government Finance (BL0102)	Underwriting – Bonds and / or Syndicated Loans and/or Cashflow / Asset Backed Securities, Privatizations & Disposals	BL0102
	Advisory services (BL0103)	Strategic planning in terms of Balance Sheet restructuring – acquisitions / disposals, establishment of subsidiaries for financial optimization, Tax Planning	BL0103
Trading & Sales (BL02)	Sales (BL0201)	Fixed income, equity, foreign exchanges, commodities, credit, funding, own position securities, lending and repos, brokerage, debt, prime brokerage	BL0201
	Market Making (BL0202)		BL0202
	Proprietary positions (BL0203)		BL0203
	Treasury (BL0204)		BL0204
Retail Banking (BL03)	Retail Banking (BL0301)	Retail lending and deposits, banking services, trust and estates	BL0301
	Private Banking (BL0302)	Private lending and deposits, banking services, trust and estates, investment advice	BL0302
	Card Services (BL0303)	Merchant/commercial/corporate cards, private labels and retail	BL0303
Commercial Banking (BL04)	Commercial Banking (BL0401)	Project finance, real estate, export finance, trade finance, factoring, leasing, lending, guarantees, bills of exchange, other loans, deposits	BL0401

Payment & Settlement (BL05)	External Clients only (BL0501) (Note: Payment & Settlement losses related to bank's own activities would be incorporated in the loss experience of the affected business line.	Payments and collections, funds transfer, clearing & Settlement	BL0501
Agency Services (BL06)	Custody (BL0601)	Escrow, depository receipts, securities lending (customers) corporate actions	BL0601
	Corporate Agency (BL0602)	Issuer and paying agents	BL0602
	Corporate Trust (BL0603)		BL0603
Asset Management (BL07)	Discretionary Fund Management (BL0701)	Pooled, segregated, retail, institutional, closed, open, private equity	BL0701
	Non-Discretionary Fund Management (BL0702)	Pooled, segregated, retail, institutional, closed, open	BL0702
Retail Brokerage (BL08)	Retail Brokerage (BL0801)	Execution & Full service	BL0801
Cost Centers/ Centralized Functions (BL09)		HR, IT, Finance & Accounts, Head Office etc.	BL0901

Individual Involved :

Individual Involved	Codes
Staff	01
Customer	02
Related Party with control/significant influence	03
Others	04

Loss Identification Number

An eleven (11) - digit code will be assigned to each loss reported based on following.
List for Bank/DFI codes is enclosed.

(00)	(0000)	(00)	(000)
Bank	Branch	Year	Case serial No. Specific for each branch

LIST OF SCHEDULED BANKS/DFIS

Code No.	BANK NAME
01	NBP
02	HBL
03	UBL
04	MCB
05	ABL
06	IDBL
07	PPCBL
08	ZTBL
09	FWBL
10	BANK AL-HABIB
11	ASKARI BANK
12	BANK ALFALAH
14	SAMBA
16	FAYSAL BANK
17	KASB

18	MEEZAN BANK
19	HMB
20	NIB
21	HBFC
23	SILK BANK
24	SONERI BANK
26	BANK OF KHYBER
27	BANK OF PUNJAB
29	ALBARAKA
30	BANK ISLAMI
31	BANK OF TOKYO
32	CITIBANK
33	DEUTSCHE
34	DUBAI ISLAMIC
35	HSBC
36	HSBC Bank OMAN
37	SUMMIT
38	STANDARD CHARTERED
39	JS BANK
40	PKIC
41	PLHC
42	POICL
43	SME BANK
44	SPIACO
45	ICBCL
46	SINDH BANK
47	BARCLAYS
48	BURJ BANK
49	PAK CHINA
50	PAK BRUNEI
51	PAIR