BEST PRACTICE GUIDELINE

From the Banking Regulation and Supervision Agency:

GUIDELINE ON OPERATIONAL RISK MANAGEMENT

FIRST PART

Objective And Scope, Definitions

Objective And Scope

1. The objective of this guideline is to declare the best practices expected from banks about operational risk management persuant to the article 35 entitled "the objective of risk management and the establishment of risk management system" of Regulation on Internal Systems and Internal Capital Adequacy Assessment Process of Banks published in the Official Gazette dated July 11, 2014 Nr:29057

2. The guideline is prepared on the basis of the Article 93 of Banking Law Nr:5411 dated October 19, 2005 and the Article 7/A entitled "Best Practices Guidelines" of Regulation on Procedures and Principles For Supervision by the Banking Regulation and Supervision Agency published in the Official Gazette dated July 22,2006 Nr:26236.

3. In accordance with the principles in this guideline, an effective and sufficient operational risk management is considered to consist of the following components considering the bank's size and complexity;

a) Operational risk management framework,
b) Organizational structure,
c) Risk culture,
d) Strategy, policy and procedures,
e) Operational risk management process
f) Business continuity

4. The principles in this guideline are prepared as a reference to effectively implement and establish operational risk management systems. Banks should consider these principles in accordance with their capital adequacy, risk profile and risk appetite.

5. Operational risk is considered on a broad perspective. Banks are supposed to develop operational risk management implementations by considering a variety of factors such as overlooking the errors and irregularities caused by flaw of the internal control, not acting according to the time and conditions, errors in bank management and information technologies and losses caused by disasters like earthquake, flood and fire. But it can be considered that there may be other operational risk factors on the basis of bank or industry mentioned above. Banks should periodically review internal and external factors affecting their operational risk levels.

Common industry practice for sound operational risk management relies on a method called three lines of defense approach. These are (i)Business Line Management (ii)Independent Corporate Operational Risk Management Function (iii)Independent Review

Depending on the size and the risk profile of a bank's activities, the degree of formality of how these three lines defense are implemented will vary. Business line management is responsible for managing and identifying the risks inherent in the products, processes, activities and systems for which it is accountable.

Independent corporate operational risk management function complements the business line's operational risk management activities and the degree of independence of corporate operational risk management function differs according to the bank's size. For small banks, independence may be achieved through separation of duties and responsibilities and independent review of processes and functions by persons except executants. In larger banks, corporate operational risk management function is responsible for the design, maintenance and ongoing development of the operational risk framework within the bank. This function may include the operational risk measurement and reporting processes, risk committees and responsibility for board reporting. Internal control as organization units or as in terms of business lines in banks is an important component of the corporate operational risk management function.

The independent review of these three lines approach may be done by competent and appropriately trained persons internal audit or suitably qualified external parties.

As discussed in the Basel Committee's paper Operational Risk -Supervisory Guidelines for the Advanced Measurement Approaches, independent review includes the following components:

Verification of the Operational Risk Framework is done on a periodic basis and is typically conducted by the bank's internal and/or external audit, but may involve other suitably qualified independent parties from external sources. Verification activities test the effectiveness of the overall framework, consistent with policies approved by the board of directors, and also test validation processes to ensure they are independent and implemented in a manner consistent with established bank policies.

Model Validation ensures that the quantification systems used by the bank is sufficiently robust and provides assurance of the integrity of inputs, assumptions, processes and outputs. Specifically, the independent validation process should provide enhanced assurance that the risk measurement methodology results in an operational risk capital charge that credibly reflects the operational risk profile of the bank. In addition to the quantitative aspects of internal validation, the validation of data inputs, methodology and outputs of operational risk models is important to the overall process.

A good communication among these three lines of defense function and a strong risk culture is the most important characteristic of a sound operational risk management framework.

Definitions

6. Following terms used in this guideline shall have the meanings expressly designated to them below,

a) Residual risk: Remained risk level after audit implementations and risk management actions performed for risk reduction
b) Business continuity: Implementations of banks regulated within the Article 13 of Regulation on Internal Systems and Internal Capital Adequacy Assessment Process of Banks and aiming to minimize operational, financial, legal and nominal negative effects in order to save in time or continue bank's activities on a cutback.
c) Control Environment: All the implementations and elements having a role in the operational risk management performance of a bank such as management philosophy, ethic principles, internal control process, organizational structure, policy and procedures, reporting, power/approval process and work distribution
d) Operational risk: The operational risk defined in the Article 3 of the Regulation on Measurement and Evaluation of Capital Adequacy of Banks.
e) Risk appetite: Risk appetite defined in the Article 3 of the Regulation on Internal Systems and Internal Capital Adequacy Evaluation Process of Banks
f) Risk capacity: Risk capacity defined in the Article 3 of the Regulation on Internal Systems and Internal Capital Adequacy Evaluation Process of Banks
g) Risk profile: Risk profile defined in the Article 3 of the Regulation on Internal Systems and Internal Capital Adequacy Evaluation Process of Banks
h) Senior management: Senior management defined in the Article 3 of the Regulation on Internal Systems and Internal Capital Adequacy Evaluation Process of Banks
i) Legal risk: Losses or other expenses from legal rulings and settlements incurred by the institution, whether judicial or out-of-court (such as arbitration, or claims' negotiations), or from voluntary actions (such as refunds, or discounts of future services offered to customers voluntarily, possibly without the customers lodging any complaints) undertaken by the institution.

SECOND PART

Operational Risk Management Framework

Principle - 1: Each bank should develop an operational risk management framework depending on a range of factors, including its size, nature, complexity and risk profile of its products and activities.

7. Operational risk management framework represents that operational risks are consistently and comprehensively identified, assessed, controlled, mitigated, monitored and reported. Banks form the operational risk management framework considering the following components and declare the framework in a written document.

- Organizational structure (board oversight, senior management, business lines, independent corporate risk management unit, internal control and internal audit),
- Risk culture,
- Operational risk management strategies, policies and procedures (including written work flow diagram) and
- Operational risk management process (the processes to identify, assess, monitor, control, mitigate and report operational risk)

In order to show the nature of operational risk, the Basel Committee has identified the management of operational risk as **'risk identification, risk assessment, risk monitoring, risk control/mitigation'**. As it is known there are a range of methods from simple to complex to quantify operational risk. In simple methods, risk measurement is done according to general criteria (as in the Basic Indicator Approach). In advanced method, risk quantification is done depending on the infrastructure. Regardless of bank's size, in order to state various approaches especially "Score Card Approach" instead of "Risk quantification/Measurement", "Risk Assessment" is used. So in this guideline these two concept are used as interchangeable.

THIRD PART

Organizational Structure

8. Sound operational risk management framework requires the attention and responsibility of a wide variety of organizational components. All staff should be competent about the identification and management of operational risk (e.g. a staff responsible for bank deposit should identify and report a matter that may cause an operational risk) and they should be aware of the level of bank's inherent operational risk. It is essential that each of the organizational components or staff (e.g. board of directors or internal control staff) clearly understands its roles, authority levels, and accountabilities under the bank's organizational and risk management structure. The establishment of an independent centralized risk management function can assist the Board and senior management in meeting their responsibility for understanding and managing operational risk. The components expected to take charge in operational risk management and their responsibilities are declared below.

The Board of Directors

Principle - 2. The Board of Directors should establish, approve and periodically review the framework.

9. The board of directors should oversee that the policies, processes and systems are implemented effectively at all decision levels. For example, it is necessary to form an assessment phase about the operational risk arising from the product during the product development process and to ensure that the internal control staff should act independently.

10. For forming a sound operational risk management framework, the board of directors should:

- establish a management culture, and supporting processes, to understand the nature and scope of the operational risk inherent in the bank's strategies and activities, and develop comprehensive, dynamic oversight and control environments that are fully integrated into the bank's overall framework,
- provide senior management with clear guidance and direction regarding the principles underlying the framework and approve the corresponding policies and procedures developed by senior management and periodically review the conformity of them,
- control if the senior management provide actions appropriate to policies effectively when necessary,
- regularly review the framework to ensure that the bank has identified and is managing the operational risk arising from external market changes and other environmental factors, as well as those operational risks associated with new products, activities, processes or systems, including changes in risk profile and risk appetite,
- ensure that the bank's framework is subject to effective independent review by audit or other appropriately trained parties.

11. Strong internal controls are a critical aspect of operational risk management framework and the board of directors should establish clear lines of management responsibility and accountability for implementing a strong control environment (control environment includes internal control processes, organizational structure, policy and procedures, reporting, power/approval process, ethic principles and work distribution). A strong control environment should provide appropriate independence/separation of duties between operational risk management functions, business lines and support functions.

Principle - 3. The board of directors should approve and review a risk appetite and tolerance statement on the basis of general and sub factors (e.g. business line, product, unit) for operational risk that articulates the nature, types and levels of operational risk that the bank is willing to assume and establish the system and processes for implementing these functions.

12. When approving and reviewing the risk appetite[1] and tolerance statement, the board of directors should consider all relevant risks, the bank's level of risk aversion, its current financial condition and the bank's strategic direction. The risk appetite and tolerance statement should encapsulate the various operational risk appetites within a bank and ensure that they are consistent.

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

[1] In this guideline, the term "Risk Appetite" encapsulates "Risk Tolerance" in international literature.

14. The board of directors should ensure that staff responsible for managing operational risk coordinate and communicate effectively with staff responsible for managing credit, market and other risks (including the risks resulting from the support services). Failure to do so could result in significant gaps or overlaps in a bank's overall risk management programme.

Senior Management

Principle - 4. Senior management is responsible for consistently implementing and maintaining of operational risk management framework in all of the bank's products, activities and processes consistent with the risk appetite and tolerance.

15. Senior management is responsible for establishing and maintaining robust challenge mechanisms and effective issue-resolution processes. These should include systems to report, track and when necessary, escalate issues to ensure resolution. Accordingly, senior management should constitute executive information system reports and written procedures about internal and external reporting (including information about distribution and frequency) and ensure that detailed reports are transmitted to authorities properly and in time consistent with each other. Senior management should also establish communication channels in order to get information about misconduct and deficiencies resulting in operational risk.

16. Senior management should translate the operational risk management framework established by the board of directors into specific policies and procedures that can be implemented and verified within the different business units. Senior management should clearly assign authority, responsibility and reporting relationships and ensure that the necessary resources are available to manage operational risk in line within the bank's risk appetite and tolerance statement.

17. Senior management should ensure that bank activities are conducted by staff with the necessary experience, technical capabilities and assess to resources and thus, reduce the potential operational risk level caused by staff.

18. Senior management should provide that in pricing and performance measurement of bank's various activities, operational risk factor should be considered properly. If not so, bank may take risk inappropriate to the risk appetite and tolerance statement.

19. Senior management should draw a procedure in which adopted approaches, methods and assumptions (e.g. which performance curve is used in assessing the assets) about valuation done before risk quantification and assessing the balance sheet items are written. The board of directors should approve this procedure.

Independent Corporate Operational Risk Management Function

20. It has become a leading practice of banks to manage operational risk through an independent corporate organization in a similar manner to credit and market risk. The key role of this organization is to assist the senior management in understanding and managing the operational risks and the board of directors in monitoring the risk management activities.

21. Each bank should establish a corporate operational risk management function in line with its organizational structure, size, complexity, risk profile and business line. So the bank can implement operational risk management through a special committee, unit and staff.

22. This organization performs the following roles:

- assisting senior management in setting policies and procedures concerning operational risk management and controls at consolidated and unconsolidated-level,
- monitoring bank's implementation of operational risk management policies, processes and procedures consistently and consolidated and unconsolidated reporting to the board of directors,
- measuring and assessing the consolidated and unconsolidated operational risk level of bank and informing the senior management,
- designing and implementing the bank's operational risk assessment methodology tools and risk reporting system,
- coordinating the bank's general risk management activities and operational risk management implementations,
- providing operational risk management training and advising the business units on operational risk management issues (e.g. deployment of operational risk management tools by business units) ,
- liaising regularly with internal and external audit.

Business Lines

23. The first level of three lines defense approach is business line management. Each business line management should identify the operational risks resulting from processes, activities and systems under its responsibility, inform the senior management and take appropriate actions.

24. Business line managers should ensure that related units should operate in accordance with the policies, procedures and workflow processes determined by senior management for operational risk. They should also establish necessary sub-level additional policy and procedures.

Internal Control

25. Among the best practices of operational risk management, in each business line there should be dedicated operational risk staff independent of executive unit. These staff members usually have dual reporting lines. While they have a direct reporting relationship in the business line, they can also transmit control results and identified risks to the central internal control unit and risk management unit to assure consistency of policy and tools and to provide independence of internal control unit from executive units. Their responsibilities may include development of risk indicators, determining escalation triggers, and providing reports to the board of directors and senior management. To be effective, such staff should be given sufficient authority and resources to carry out their responsibilities.

Other Operational Risk Related Functions

26. There are a number of business units having responsibility about factors affecting operational risk level of bank directly or indirectly along with the units/staff mentioned above. These include specialist units such as legal and compliance, human resources, information technology and accounting/financial reporting which should be responsible for some specific aspects of operational risk or units responsible for issues indirectly leading risks. These other operational risk related functions should on the one hand be responsible for managing the operational risk in their own area and on the other hand provide information and support to other units about operational risk types, levels and management. For example on a credit assignment process, bank's accounting unit may be responsible for identifying an operational risk caused by the wrong accounting treatment of accounting staff.

Role of Internal Audit

27. Internal audit is responsible for independent assessment of operational risk management framework in all its parts.

28. Internal audit units should have in place adequate audit coverage and resources to verify that operational risk management policies and procedures have been implemented effectively across the bank. The board of directors should ensure that the scope and frequency of the audit program designed by the internal audit unit is appropriate to the operational risk level the bank is exposed to. Any operational issues identified and reported in the audit process should be addressed by the senior management in a timely and effective manner or raised to the attention of the board of directors, as appropriate.

FOURTH PART

Risk Culture

Principle - 5. Banks should ensure that a strong risk culture across the bank is established through operational risk management function. The board of directors and the senior management should take the lead in meeting this liability, recognize the main factors of the operational risk and consider this risk as a different risk category to be managed.

29. The policies, procedures and systems, on-the-job trainings and effective internal control unit will provide the foundation of a strong corporate culture that is guided by risk management in the bank and the integration of operational risk management culture to all units and activities. Banks with a strong culture of risk management are less likely to experience potentially damaging operational risk events and are better placed to deal effectively with those events that do occur.

30. The board of directors should establish a code of conduct or an ethics policy and identify compensation policies in a bank. Clear expectations and accountabilities ensure that bank staff understand their roles and responsibilities as well as their authority to act and prohibit conflicts. Strong and consistent senior management support for risk management has critical importance in getting expected utility. Compensation policies should be aligned to the bank's statement of

risk appetite and tolerance, financial goals and long-term strategic direction. They should also appropriately balance risk and reward.

31. The bank's business, risk management activities and controls should be conducted by qualified staff with the necessary experience, technical capabilities and adequate access to resources to ensure the continuity of a risk culture in the bank

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

33. There must be an environment in which staff can speak out and raise operational risk problems openly without fear of negative consequences.

34. The required infrastructure in data processing unit or intranet should be set to inform the staff about operational risk policies and procedures and should be always available for staff.

FIFHT PART

Strategy, Policy And Procedures

35. Operational risk management process begins with the determination of the overall strategies and long-term objectives of a bank. Once determined, the bank can identify the associated inherent risks in its strategy and objectives, and thereby establish an operational risk management strategy and develop an operational risk management framework appropriate to all these strategies. The risk appetite of the bank and basic elements regarding its management should be determined and documented in the operational risk management frame work.

36. The directors of each unit in bank are responsible for managing risks in their particular business units. Therefore, all business units[2] are required to develop supplementary policies and procedures specific to their business based on and in consistence with the corporate operational risk management framework. It has great importance to establish written work flow diagrams within the procedures. There is not a standard format about the scope and shape of these diagrams but they should be established in an easily understandable detail and style.

An example of determining operational risk strategies, policies and procedures and corporate strategy of a bank is mentioned below.

The corporate strategy of the bank is determined by the board of directors as 20% growth of assets each year in a three year perspective. According to calculations, the bank shall have an average 13% of CAR per year for attaining this objective. So, the bank's risk appetite is at a level of minimum 13% of CAR. The board of directors has decided that capital requirement of operational risk should not be over 15% of total requirement and has given instructions to the head office for this. (These are a typical example of establishing corporate strategy and operational risk strategy process)

The head office has developed risk policies in order to avoid operational risk exceeding the stated level in accordance with the determined strategy and has decided to make insurance for financial losses resulting from for example an error in assessing the credibility of customer during the assignment of a credit card. (It is assumed that the

[2] F

37. A corporate policy and procedures established considering the operational risk management framework should include the following components.

- The operational risk types that are faced before or have the potential to be faced by the bank (a common taxonomy of operational risk terms should be established in order to ensure consistency of identification, rating and management of risks. If the bank does not adequately identify and classify operational risk and loss types, the quantification and management of risks may be prevented),
- Rules about issues like approving of new customer, product and information management systems, using support services, business continuity plans, crisis management and money laundering which are the components of operational risk,
- The organization structure used to manage operational risk, including reporting lines and responsibilities (for example, the report control authority, identification of signing and transmission procedures),
- The risk assessment and measurement methods and how they are used
- The limits for inherent and residual risks as part of the bank's operational risk appetite and tolerance in the strategy document, approved mitigation strategies and other related issues,
- The process of monitoring limits for inherent operational risks of bank,
- Management Information Systems (MIS) used in risk reporting and monitoring process,
- Processes ensuring the assessment of operational risk by independent groups (these processes include establishing an information system, avoiding "black box" approach, considering archiving and succession important)
- The process of updating or reviewing policies whenever a material change in the operational risk profile of the bank occurs (for example; the bank grows by 20 %while the sector's average growth is 10%,)

  The Basel Committee defines operational risk as inadequate and unsuccessful internal processes, loss risk resulting from external issues or staff and systems. The table on the following page provides an example of risk cause categories in four parts:

Basic Risk Factors	Examples
Processes	• Inadequate / inappropriate guidelines, policies and procedures • Lack of / failure of communication • Erroneous data entry • Inadequate reconciliation • Poor customer / legal documentation • Inadequate security control • Breach of regulatory and statutory provisions / requirements • Inadequate change management process • Inadequate back up / contingency plan
Staff	• Breach of internal guidelines, policies and procedures • Breach of delegated authority and neglect of duty • Internal criminal acts • Inadequate segregation of duties / dual controls, inexperienced staff • Staff oversight and unclear roles / responsibilities
System	• Inadequate hardware / network / server maintenance
External Issues	• External criminal acts • Vendor misperformance • Man-made disaster • Natural disaster • Political and legislative causes

SIXTH PART

Operational Risk Management Process

Principle - 6 Banks should have a risk management process and appropriate means to be able to regularly identify, measure, assess, monitor and control the operational risk exposure due to their products, activities, processes and systems.

Risk Identification, Measurement, and Assessment

Principle - 7 Senior management is responsible for identification and assessment of operational risks of all important products, activities, processes and systems.

38. Each bank, with the aim of identifying operational risk profile in the most correct way and by this way to be able to assign its sources to the risk management optimally, first of all, should identify their various risk exposure types as concrete as possible and assess its fragility level due to above-mentioned risk types. Effective identification, measurement and assessment are

of vital importance in obtaining expected results from monitoring and control processes which constitute the subsequent stages in risk management.

39. In the process of identifying operational risk, it is important to consider internal and external factors which negatively affect the bank activities, sufficiently in scope and content. For example, some of the above-cited factors are:

- the bank's management structure, risk culture, human resource management approaches and practices, organizational changes and employee turnover;
- the bank's customer, product, and service profile, the nature of the service distribution, and the complexity and volumes of transactions;
- constructed work flows related to each product and the service that the bank offers to its customers, and the process of their implementation; and
- the effect of political, legal, technologic and/or economic changes on the bank's business frame of activities, sectoral trends, competition level, and market structure.

40. Following the identification of risk the bank should define appropriate approaches within the context of the measurement of identified risks and assessments, also should estimate the probability that the identified risks will materialize by considering the causes of the risks and assess their potential effects on the bank's current activity volume, structure, and targets.

41. Some of the tools that the bank may use for identification, measurement, and assessment of the operational risk include:

(a) Audit findings: Findings obtained from internal and external auditing primarily focus on control weaknesses and security flaws while on the other hand they are important inputs for the identification process of the operational risk exposure level;

(b) Internal Loss Data Collection and Analysis: Operational loss data provides significant inputs in identification of internal control efficiency and operational risk exposure level of a bank. The analysis of loss events provides information about the reasons of losses, for instance, makes it clear as to whether the control errors originate from the mistake related to the events or from a systematic mistake;

(c) External Data Collection and Analysis: External data consist of gross operational loss amounts occurring at organizations other than the bank, dates of the losses, compensation amounts (collected from insurance, personnel etc.), and reasons for the losses. Comparison between external loss data and internal loss data can be used to explore possible weaknesses in the control environment of the bank or identify previously unidentified risk factors;

(d) Risk Assessments: A bank's self-assessment related to the operational risk includes potential threats originated from activity processes and activities and the assessment of vulnerabilities by the bank against the threats as well as the analysis of the possible negative effects of the threats and vulnerabilities on the bank. Besides, the bank should assess the risk control process (risk control process consists mainly of the controls directly applied by the business lines and internal control unit's applications). In this context the bank assesses the risk

level previous to control, reviews the efficiency of the control environment and indicates the residual risks (residual risk factors after control). Residual risks can be weighted by the bank and for this purpose scorecards can be used. This system, by enabling the assessment results to be translated into metric system, will offer an opportunity of rating related to the control environment;

(e) Business Process Mapping: Business process map is a form, starting from the most general class, shows the overall process of the product/service and connecting points in the work flow diagrams all together. In this context, for instance, the bank, after defining its corporate finance activity as in the first level division (retail banking is an example of another main activity in the first level), identifies the sub-activities related to the main activity: mergers and acquisitions, securitization, mediation in issuance of securities. Work flow diagrams that indicate the methods of business and transactions performance under each sub-activity's responsibility are complementary factors of the map, as well. The bank, offering the above-mentioned maps with using software support within determined rules frame to relevant employee will increase the expected benefit of the application. With the business process map, the bank aims to determine isolated and interrelated risks, and on the other hand to reveal the weaknesses in the control and risk management functions. The bank, by using the map, will be able to see the principal stages in the business processes and other organizational activities in the common ground and by this means will be able to identify the principle risk points in the bank processes. This method will also be helpful in determining priorities of the management actions in the following periods;

(f) Risk and Performance Indicators: Risk and performance indicators are the risk metrics and/or statistics that provide the risk factors analysis of a bank's risk exposure. Quantities in indicators and changes displayed by these quantities in time are highly useful in identifying operational risk and assessment process (e.g. data related to the bank's operational efficiency level, consent errors, employee turnover, system disruptions, transaction volumes and number of errors, audit scores, number/rate of activity areas left out of audit, limit breaches). Risk indicators are used in monitoring possible factors related to principle risks. As to performance indicators, they provide significant information about operational weaknesses, current situation of business processes and experienced error and losses. Both of the indicators operate as warning mechanisms when risk levels are close to threshold/limits or exceed, and in triggering levels that require urgent risk mitigation;

(g) Scenario Analysis: A bank, by obtaining opinion from the experts and risk managers in business lines, should develop scenario analyses with the aim of identifying operational risk events and assessing their potential outcome. Analyses are effective tools in determining potential risk factors, additional controls or requirement for risk mitigation. Given the subjectivity of scenario analyses, additional measures will be appropriate to be taken by the bank in order to ensure the efficiency, consistency, and objectivity in analysis process. Extensive explanations related to the scenario analyses that the bank will give place to in risk management implementation are in the "Guideline on Stress Tests to be Used in Capital and Liquidity Planning of Banks"

(h) Measurement: The bank may quantify its exposure to operational risk level by using the outputs of the risk assessment tools (internal loss data, audit findings, scenario analyses etc.) as inputs into a model that measures the operational risk. The results of the model can be used in the bank's economic capital calculation and can be allocated to business lines to link risk and return.

In order to quantify the risk, a bank that adopted an advanced calculation method should completely/correctly collect the historical data related to operational loss events and identify potential sources that caused operational loss. Data base established by the bank about the loss events can be used in empirical analysis, and modeling and quantification of the associated loss events;

(i) Comparative Analyses: This kind of analysis is based upon comparing the results of the various assessment tools to provide a comprehensive assessment related to the bank's risk profile. E.g. the risk level that the bank may be exposed to can be seen more easily by comparing data used for scenario analysis with internal and external data.

Risk Monitoring and Reporting

Principle - 8: Banks should establish process and system to regularly monitor their operational risk profiles and exposure to losses.

42. This process should include the implementation of qualitative and quantitative assessment of the bank's exposure to all types of operational risks, the assessment of quality and appropriateness of corrective/mitigation actions, ensuring that adequate controls are in place (e.g. whether the current control level enables it to identify problems before the bank's losses become major concerns). The process, at the same time, should be appropriate to the bank's scale, risk profile and activity nature.

43. In monitoring its operational risks, the bank should develop appropriate indicators that provide management with early warning of operational risk issues (often referred to as "key risk indicators" (KRIs). The indicators, by providing predictive information related to the bank's exposure to the potential risks and explaining the potential sources of the risk, enable the bank to take necessary actions before the bank is exposed to important losses. In identifying KRIs, the bank utilizes a pool that consists of the bank's various functions, control processes and all activities. The indicators are regularly monitored by various business lines of the bank. Established as principal indicators, targets and limits or escalation triggers will allow the breakdown in risk management and potential problems to be negotiated with the bank's senior management by operating as an early warning function in monitoring process related to the increase in operational risk level (other preventive application examples of early warning mechanisms for abuses: the daily central controls of accounts , controls of provisional accounts, controls of the credits given to the same person in the same day).

44. Monitoring process of the operational risk, should be integrated with the bank's routine activities and in this context the operational risk potential of each business line should be

assessed, in this assessment process the frequency and nature of changes in the operating environment should also be taken into account.

45. Within the context of monitoring the operational risk, a report should be prepared to be submitted to the Board and this report should, as far as possible, contain the relevant internal financial and operational data, the level of the bank's compliance with legal and internal regulations and information needed during decision making about the external market conditions. The principal aim of this kind of reporting is to provide various information enabling the management to understand the operational risk profile and its effects thoroughly. In this report, the points that aim especially to inform the Board, senior management and relevant business lines, are listed as follows:

- the critical operational risks facing, or potentially facing the bank (e.g. negative changes that indicated by KRIs directly or by the trend analysis, assessments in audit/compliance reports);
- major risk events/loss experience, issues identified and intended remedial actions;
- the strategies of mitigation and transformation of the risk;
- the status and/or effectiveness of actions taken;
- the information related to operational risk originated from new products;
- the identification of weak areas;
- the distribution of the operational risk amounts among the business lines, their course and gradations;
- exceptional reporting (authorized and unauthorized deviations from the bank's risk appetite, risk capacity, and risk policy and likely or actual breaches in predefined thresholds for operational exposures and losses); and
- the likely effects of major external events and their effects on the bank and on its operational risk capital.

All results of a bank's risk monitoring process, findings identified by internal control, internal audit and/or the risk management function, the reports prepared by independent external auditor and audit authority, as appropriate, should be included in the operational risk management/monitoring reports.

Reports will regularly be received from areas that have a role within the context of posing a risk and its management such as business units, support functions, the operational risk management function and internal audit, by senior management, to be used in the forming process of the above-cited reporting process and the report to be submitted to the Board. ,. Senior management should ensure that regular management reports on operational risk are received by relevant level of the management, on a timely basis and business areas are monitored by the relevant personnel by means of the reports and also the points of critical importance are negotiated at the Board level.

46. Frequency or timing related to reporting, should be planned on a need basis, additional reporting opportunity should also be provided in conditions subject to stress. Bank scale, complexity in the activity nature, structural features of the risk, and frequency of change in the activity setting should be taken into consideration while identifying reporting frequency. However, in any case, reporting in terms of the bank's activity volume, nature and/or complexity, at least in quarterly or semi-annually is necessary on an ongoing basis.

47. The bank's current reporting and data collection processes should regularly be reviewed for remediation of the current risk management performance and improvement in the policy, procedure and implementations of the risk management, and in this regard, the best practices should be followed.

48. Bank's senior management should ensure that reporting related to the operational risk management is accurate, consistent, and usable. In this manner, reports should be considered carefully so as to be appropriate in scope and volume, data should not contain a possibility of failure in taking decision effectively for being insufficient or overloaded. To ensure the received reports are directed towards the goals and reliable, senior management should regularly review the compliance of reporting system constructed in the bank, with the timing table, whether they provide complete/correct information, the consistency of information under the same headings in the reports prepared by different units, that the reports are delivered to relevant authorities in time, its compliance with the bank's scale and risk profile, and the statistics related to the internal control activities.

Risk Control and Mitigation

Principle - 9 Banks, by utilizing prepared policies, processes and systems, have to constitute a strong operational risk control and mitigation process with internal controls, risk mitigation and/or transfer strategies.

49. Internal controls fulfilled by the bank should provide means to make the bank's operations productive and efficient; minimize personnel flaws; safeguard the assets; produce reliable financial reports; and comply with applicable laws and regulations.

50. Control processes should contain various implementation (e.g. reports of difference that deals with inconsistencies between transactions made in any business process and predicted transactions in the procedure related to the business process in the question) that increase the compliance level with the bank's policies. In the context of the policy compliance level assessment, it will be useful to consider the following points.

- following the ongoing process of stated objectives continually by the senior management;
- reviewing the progress made through the measures and solutions to the points failed to comply, by senior management;

- reviewing of the required authorization and approval processes periodically to provide accountability to relevant level of management; and
- establishing an effective reporting process to track exceptional implementations in threshold values and limits or other deviations from policy, conscious/unconscious.

51. An effective control environment, to the highest degree possible, requires segregation of duties in the bank and establishment of crosswise control points. Because, assignments that establish conflicting duties for individuals or without control process (or other countermeasures) may enable concealment of losses, errors or other inappropriate actions. Therefore, areas of potential conflicts of interest should be identified, minimized, and be subject to careful independent monitoring and review.

52. The bank should ensure that its risk management control infrastructure keeps pace with growth or changes in the business activity and increasing complexity (e.g. new products, branches/subsidiaries remote from head office, and entry into unfamiliar markets).

53. Typical practices to control operational risk in a bank consist of the following factors:

- effective segregation of duties to avoid a conflict of interest in the responsibilities of individual staff which can facilitate concealment of losses, errors or inappropriate actions and clearly planned authorizations and approval processes;
- close monitoring of adherence to assigned risk limits or thresholds and investigation of breaches;
- an effective authorization and security process for access to, and use of, bank assets and records;
- for providing and maintaining specialization at all levels of the bank's activity, appropriate personnel selection and improving training opportunities (providing the staff of equal seniority and similar activities with equal time and similar training should also be considered within the context in question);
- training documents prepared for activities applied in the bank should be contained in the data processing system to provide an easy access, and be updated regularly;
- identifying business lines or products where returns appear to be considerably out of line with the expectations (e.g. where a supposedly low risk, low margin trading activity generates high returns must be subject to a research whether such returns have been achieved as a result of an irregularity or internal control weakness);
- regular verification and reconciliation of transactions and accounts; and
- a permission-and-proxyship policy aiming to fulfill the responsibilities of an absent personnel because of various reasons.

54. After identifying its operational risk exposure, the bank, first of all, determines its strategies against the above-cited risks. In this process, each bank should determine an appropriate choice whether to control risk exposure by implementing projected policy and procedures, to mitigate using risk mitigation techniques, to transfer to another sector or area, to prefer alternative risk

sorts (e.g. legal or counterparty risk) or to carry it as it is. For those risks which can not be controlled or mitigated, the bank should assess as to whether to accept these risks, reduce the level of business activity involved, or withdraw from this activity completely.

55. The bank can transfer certain level of their operational risks to third parties through risk mitigation products such as insurance. However, using tools of risk mitigation instead of internal operational risk controls is not a correct approach.

Special Aspects for Consideration

56. The bank should have policy and procedures of special quality for the following factors.

- **New products and activities**

57. Operational risk level rises significantly when the bank interferes new sorts of activities or develops new products and especially when these activities and products are strange to the bank's basic activity nature. Therefore, the bank's new product/activity approval processes, in certain standards, should be based on written policies and procedures, and duties and responsibilities for product/activity should clearly be identified. The basic purpose of prepared policies and procedures is to realize the change in the nature of new business initiatives or current activities in a controlled manner and to prepare relevant business units and support functions for implementation process.

58. Sorts and levels of possible risk exposure due to the bank's new products, activities, processes and systems should be assessed and they should be materialized after the assessment. The assessment and approval process, at least, should clarify the following points.

- What are the possible risks of new product, service, and activity?
- What are the difficulties that may arise in the evaluation of new products and how might these evaluations change during the stres periods of the economy?

- What kind of changes will it create in the bank's current operational risk profile, risk appetite and risk capacity?
- What are the appropriate control and risk management processes and risk mitigation strategies?
- What are the residual risks after control?
- Should any change be made in relevant threshold values or limits?
- What are the procedures and methods of measurement to be used in the risks caused by new product and activity?

- **IT capacity and security and change of IT systems, facilities and equipment**

59. Using information technologies (IT) facilities widely, provides significant contributions to the bank in having an effective control environment because automatized processes, compared to manual ones, minimize the error risk significantly. On the other hand, technologic infrastructure used in product presentation, activities and processes or channel of service distribution, at the same time, causes the bank to be exposed to strategic, operational, credibility etc. risks and financial losses. For this reason the bank, by following risk management programs belonging to technologic risk management and infrastructure, should identify, measure, monitor and, by using various tools, manage the risk factors caused by use of technology and automatized processes. Technologic risk is managed by the similar approaches to operational risk management and should include the following factors.

- including received support services, management and control implementation providing consistent improvement with current nature and targets of the bank's technologic infrastructure;
- creating expectations of risk appetite, capacity, and performance to provide support for risk management and control;
- identifying the policies and procedures that provide opportunity for identification and assessment of risks;
- within the context of policies and procedures, establishing an effective control environment and manifesting transfer-mitigation strategies to be implemented when necessary; and
- monitoring the adherence level to identified threshold values and limits.

60. Policies and procedures prepared within the context of technology risk management primarily aims to manage through the effective IT controls of risks that the bank is exposed to due to its IT infrastructure, security management, system development and change management, information processing, communication network, and technology service providers.

61. The bank's senior management, along with the activity level under normal conditions, will ensure that the activity under stressful conditions also will not be hindered, on the other hand it is responsible for providing a technologic infrastructure with sufficient capacity for current and long term activity planning. This infrastructure should provide opportunity for providing necessary data, system integration/security, access to the system in time, extensive risk management and submitting information required by authorized third parties, resiliently and in a desired form and content. Besides, dealing with operational risks regularly by third parties, through independent IT audits is highly important for risk management.

62. Banks are heavily exposed to operational risk due to partial, disconnected, cost-cutting or insufficient technologic infrastructure which occurs during the processes of mergers and acquisitions in a bank. Factors causing operational risk will primarily hinder dealing with the

risk in various dimensions by making it difficult to collect necessary information from consolidated institutions and/or activity areas and to analyze, on the other hand it will disrupt risks management and monitoring especially in high growth periods. For this reason, bank management should operationalize the secure technologic infrastructure before completing merger operations by assigning appropriate capital or implementing high growth strategies and presenting new products to customers.

- **Alternative distribution channels**

63. Management of the risks originated from alternative distribution channels (ATM, internet banking, online banking etc.) constitute an inseparable part of the bank's technologic risk management. This stage contains customer safety implementation, and other exclusive controls aiming risk management which are about authorization customers, confidentiality and integrity of information, implementation security, internet infrastructure, preventing unauthorized access to the customer accounts (e.g. by using fake e-mails or websites).

- **Support services**

64. Institutions that fulfill the bank's activities in the name of it, excluding agreement on deposit or participation fund, giving credit in cash, non-cash, all other sorts, and transactions accepted as credit by the legislations; or that serve as assistant to the bank in commercializing even one of the activities out of advertising and acceptance of deposit and participation fund, are accepted as support service providers. This kind of service, along with substantial cost advantage, expert support, advantages related to range widening or recovery of service, brings about a set of risks to be taken into consideration by the bank. Management of risks originated from support service includes comprehensive risk assessments through critical importance carried by the proposed service for the bank, situation assessment about service providers, service related control facilities and contingency planning. The Board and senior management are responsible for understanding the risks created by support service agreements and developing effective policies and procedures for the risks management. Service procurement policies and risk management implementation should primarily include the following factors.

- policies and procedures that identify what kind of bank activities can be subject to the support service procurement and how;
- the process to be followed in assessment study aiming the selection of potential service providers;
- establishing support service procurement agreements sturdily (the factors such as possession in agreements, credibility of information, responsibility for confidentiality, responsibilities, rights of cancellation etc. should clearly be manifested);
- implementation for monitoring risks originated from support service procurement and service providers (e.g. in order for service provider to fulfill its responsibilities the important thing is to regularly monitor its financial condition);

- developing an applicable and tested contingency plan in response to the possibility of a critical failure in support services; and
- taking opinion from law unit for preparing uniform contract appropriate in scope and content clearly identifying the responsibilities of service provider and bank and/or service procurement agreements.

65. When the bank is not able to manage the risks originated from support service procurement adequately, however cancellation of service procurement is also not a reasonable choice, the bank's senior management can transfer the risks to a third party (through insurance etc.) with the aim of eliminating its control weakness. In this case the Board, considering the bank's financial strength, identifies the maximum loss amounts that it can manage and implements the bank's risk and insurance management program. The results of the above-cited program should be reviewed at certain intervals. However, this implementation does not remove the responsibilities for the bank's Board members and managers that exist in the legislation.

- **Money laundering**

66. The bank, within the context of combating money laundering and terrorist financing, should develop policies, procedures, controls based on the principles of know your customer, compliance with laws, co-operation with law enforcement agencies, and on-going staff training.

- **Suitability of customers**

67. The bank should identify the suitable customer types to sell them certain sophisticated, high risk products and have policies and procedures containing this kind and similar factors. The target customers should be considered as capable of understanding and bearing the potential financial risks that may rise from such products which is a principle criterion that the bank should take into account.

- **Foreign branches and subsidiaries**

68. The principle banking system and activity processes of foreign branches and subsidiaries may substantially affect the bank's risk profile. Therefore, the bank should integrate current systems of the branches and subsidiaries with its main system at the highest level possible and document its activity processes in appropriate scope and content, understand the impact of the changes, and develop appropriate control mechanisms over foreign operations.

- **External documentation**

69. External documentation refers to documents that are produced by banks and provided to customers and counterparties or third parties, (e.g. contracts, transaction statements, or advertising brochures) and brings right/obligation to the bank. The presence of inappropriate or inaccurate information in these documents can lead to legal risk and/or operational risk. For

this reason, it is important for the bank to have a reviewed written control process prior to the issue of external documentation. In this control process, written opinion given by the bank's law unit constitutes the most important phase. In the above-cited reviewing process, it will be appropriate to control the documents planned to be issued, primarily on the basis of the following factors.

- compliance with legal requirements;
- the extent of standard and non-standard terms used in the documents;
- the channels in which the documents are issued;
- compliance with approving mechanism; and
- compliance of the contract with standard contact types prepared by the bank.

SEVENTH PART
Business Continuity

Principle – 10 Banks need to have a business continuity plan to be able to continue their activities on an ongoing basis and limit losses in the event of severe business disruption.

70. Banks are incessantly exposed to disruptive events, some of which may be severe and result in an inability to fulfill some or all of their business obligations. Incidents that damage or render accessibility to the bank's facilities, telecommunication or information technology infrastructures, or a pandemic event that affects human resources, can result in significant financial losses to the bank, as well as broader disruptions to the financial system altogether. Against this kind of events, each bank should establish business continuity plans considering their size, activity nature, and complexity of their processes. These plans should manifest various programs developed according to different types of likely or plausible scenarios to which the bank may be vulnerable.

71. Within the context of business continuity management, each bank should give place to impact analysis, system and data recovery strategies, testing business continuity management from various points, duty in urgent cases, distribution of authorities/responsibilities in a clearly identifiable way, training related to the implementation in the business continuity plan, programs leading increase in awareness, and communication and crisis management programs. In the above-mentioned process, a bank should primarily identify its critical activities, on the consolidated and nonconsolidated basis dependence to internal and external service types (e.g. public services like electricity/water, supplying goods, support services provided from third parties) and their appropriate resilience levels. Negative condition scenarios created by the bank should be assessed for their financial, operational and reputational impact and the resulting risk assessment should be the foundation for recovery priorities and objectives. Business continuity plans should contain contingency strategies, recovery and resumption procedures, and communication plans for management, employees, legal authorities, customer, service suppliers, and – where appropriate – communication repots for informing civil authorities.

A bank should regularly review its continuity plans to ensure contingency strategies remain consistent with current operations, risks and threats, resiliency requirements, and recovery priorities. Training and awareness programs should be implemented to ensure that staff can effectively execute contingency plans. Accordingly, the plans should be tested periodically to ensure whether recovery priorities comply with time constraint. Besides, the bank, along with service providers of critical importance, should also test disaster recovery and business continuity plans at appropriate intervals. Results of testing should be reported to the senior management and the Board simultaneously.