Standards on Risk Governance in Financial Institutions
Foreword and Acknowledgements

This manual has been prepared by IFC’s Banking Advisory Program in partnership with the Development Bank of Austria (OeEB).

The Program thanks the Association of Russian Banks and the following people for their valuable input into the report: Iveta Gigova, IFC Consultant; Anatoliy Milyukov, Deputy Chairman, Association of Russian Banks; Ferdinand Tuinstra, IFC Senior Banking Advisor; Natalia Ponomareva, IFC Banking Advisor; Denis Bondarenko, IFC Banking Expert.

About IFC

IFC, a member of the World Bank Group, is the largest global development institution focused on the private sector in developing countries. We create opportunity for people to escape poverty and improve their lives. We do so by providing financing to help businesses employ more people and supply essential services, by mobilizing capital from others, and by delivering advisory services to ensure sustainable development. For more information, visit www.ifc.org.

The findings, interpretations, and conclusions expressed in this study are entirely those of the author, and should not be attributed in any manner to the World Bank or IFC, to its affiliated organizations, or to members of its Board of Executive Directors or the countries they represent. Dissemination of this study is encouraged and IFC will normally grant permission promptly. This paper was issued by IFC in English and Russian. For questions about this report, including permission to reprint portions or information about ordering more copies, please contact IFC.

About OeEB

Oesterreichische Entwicklungsbank AG (OeEB - the Development Bank of Austria) is a wholly-owned subsidiary of Oesterreichische Kontrollbank AG (OeKB), the Austrian export credit agency, and has an official mandate from the Government of Austria to act as official development bank. OeEB is specialized in realising private-sector projects that require long-term financing and that can service their borrowings out of their own cash flow, and have a sustainable impact on the regional economic development. More info on www.oe-ebr.at

Copyright © 2012 International Finance Corporation
# TABLE OF CONTENTS

## GENERAL PROVISIONS ......................................................................................................... 5

## INTRODUCTION ..................................................................................................................... 6

### I. KEY PRINCIPLES OF SOUND RISK GOVERNANCE ..................................................... 7

#### 1. RISK APPETITE DETERMINATION .................................................................................. 7

   1-A Some Background on the Fundamentals of Financial Risk and its Theory ............ 7
   1-B Difficulties in Determining Risk Appetite ................................................................. 7
   1-C Components of the Risk Appetite Determination Process ........................................ 8
   1-D Apportioning and Communicating Risk Appetite down throughout the Bank........... 9
   1-E Communicating Risk Appetite Externally ................................................................. 9

#### 2. RISK-BASED INCENTIVES AND COMPENSATION ..................................................... 9

#### 3. CONFLICT OF INTEREST ELIMINATION ..................................................................... 10

   3-A Independence, Segregation of Duties ....................................................................... 11
   3-B External Validation ...................................................................................................... 12

#### 4. PERVASIVE RISK CULTURE .......................................................................................... 13

   4-A Accountability, Disclosure, Transparency ............................................................... 13
   4-B High Ethical Standards ............................................................................................... 13
   4-C Important Risk Awareness Behaviors ....................................................................... 13

#### 5. EFFECTIVE COMMUNICATION .................................................................................... 14

#### 6. STRONG CHIEF RISK OFFICER AND RISK FUNCTION ............................................ 14

#### 7. STRONG RISK COMPETENCIES .................................................................................. 15

### II. ORGANIZATIONAL STRUCTURE and KEY PARTICIPANTS .....................................16

#### 1. THE BOARD ................................................................................................................ 16

   1-A Composition and Selection ....................................................................................... 17
   1-B Clear Mandate and Accountability ............................................................................ 17

#### 2. BOARD RISK COMMITTEE .......................................................................................... 17

#### 3. BOARD AUDIT COMMITTEE ....................................................................................... 18

#### 4. CHIEF EXECUTIVE OFFICER ..................................................................................... 18

#### 5. CHIEF RISK OFFICER ................................................................................................ 18

#### 6. CREDIT COMMITTEE .................................................................................................. 19

#### 7. ASSET AND LIABILITY COMMITTEE (ALCO) ............................................................. 19

#### 8. THE DEDICATED RISK FUNCTION ............................................................................. 19

#### 9. CHIEF FINANCIAL OFFICER ...................................................................................... 20

#### 10. INTERNAL AUDIT .................................................................................................... 20
11. LEGAL and COMPLIANCE FUNCTIONS ................................................................. 20
12. EXECUTIVE OFFICERS, INDIVIDUAL BUSINESS UNITS, ALL STAFF ............. 21

III. THE RISK MANAGEMENT PROCESS ................................................................. 22

1. OVERVIEW ............................................................................................................. 22
2. IDENTIFICATION ..................................................................................................... 22
3. ASSESSMENT / MEASUREMENT ......................................................................... 23
   3-A Exposures ........................................................................................................... 23
   3-B Sensitivities ....................................................................................................... 23
   3-C Probabilistic Measures ...................................................................................... 23
   3-D Scenario Analysis / Stress Testing .................................................................... 23
   3-E Risk Models ....................................................................................................... 24
   3-F Additional Considerations ................................................................................ 24
4. CONTROL / MITIGATION ...................................................................................... 24
   4-A Limits and Other Mechanisms .......................................................................... 24
   4-B New Product Approval ...................................................................................... 24
5. MONITORING / REPORTING / COMMUNICATION/ EVALUATION .................. 25

CONCLUSION ............................................................................................................. 26

Appendices .................................................................................................................. 27
Appendix 1: Evaluation Table – Key Risk Governance Principles ......................... 28
Appendix 2: Evaluation Table – Risk Management Organizational Structure .......... 34
Appendix 3: Evaluation Table – Risk Management Process and Practices ............. 37
Appendix 4: Terms and Definitions .......................................................................... 40
Appendix 5: References ............................................................................................. 42
These “Standards on Risk Governance in Financial Institutions” (hereafter - the “Standards”) discuss a set of corporate governance principles that constitute current best practice in risk governance. Some of those principles are well established and broadly applicable in general corporate governance best practice while others have a narrower application to banks. Although the document is geared specifically to banking organizations, many of the concepts presented are relevant to other financial institutions.

In addition to the key principles of risk governance, this document also outlines the organizational structuring commonly found in banks today for managing risk, as well as a conceptual risk management framework and its main elements. Within this framework, emphasis is placed on risk assessment and on related best practice.

The key objectives of these Standards are as follows:

- To improve the effectiveness of risk management and control within financial institutions.
- To enhance standards of risk management within the banking sector, thus raising confidence among the wider public and business.
- To enhance the competitiveness and financial sustainability of financial institutions (and, ultimately, their general stability) by implementing risk governance standards consistent with national and international best practice.

The key stakeholders most likely to benefit from these Standards are as follows:

- **Financial Institutions.** Implementing these Standards will enable small and medium-sized banks to improve their risk management processes; enhance their financial sustainability, efficiency, and competitiveness; and improve the reputation (and the public’s perception) of their own bank.
- **The clients of financial institutions.** Implementing these Standards will give commercial bank clients better access to information on their own bank’s risk management policies, enabling them to take a better-informed and independent view of their bank’s viability and stability.
- **The governance and management bodies of financial institutions** (i.e., shareholders, the Board of Directors, and senior management). Implementing these Standards requires complete commitment to best practice in corporate governance, and, specifically, to best practice in risk management. Meeting such standards, as well as ensuring effective internal regulation and control, will improve business management and profitability and help to avoid unexpected losses and corporate disputes.
- **Banking regulators.** As well as improving corporate governance, implementing these Standards will enhance the competitiveness of commercial banks, as well as their ability to adapt to market conditions, ensuring better protection for creditors and depositors and promoting the greater financial sustainability of the banking system as a whole. Regularly assessing risk management framework of financial institutions, as well as their broader viability and financial standing, will ultimately result in a more streamlined and differentiated regulatory environment.
- **Government agencies.** Insofar as it helps financial institutions to meet their obligations, best-practice in risk management is conducive to economic growth.
INTRODUCTION

The field of risk is inherently complex. Additional complexity has resulted from the rapid development of financial markets, products, and financial services organizations over the past two decades, and the concurrent accumulation of a large body of thought and vast amounts of regulation on risk topics. This has sometimes had the unintended consequence of obscuring, rather than illuminating, the underlying rationale of risk management.

Sound risk governance requires that fundamental principles be understood in their depth and applied in spirit, rather than mechanistically following rules and regulations. This document seeks to aid this understanding through examining behaviors and revisiting fundamental reasons for some of the common practices in the risk profession. It is hoped that this approach will facilitate practical understanding and meaningful implementation.

Outlining standards and degrees (or stages) of their implementation helps organizations to measure their own level of achievement in the area of risk governance, both against best practice and against their peers. Such standards allow Boards, bank executives and risk managers to identify gaps and design improvements. The standards can also be helpful to external parties, such as regulators, investors, auditors, rating agencies, and others, in assessing and comparing different institutions.

Risk governance principles are, above all, the responsibility of the Board of Directors and of the most senior executives and management bodies of a banking institution. The members of those bodies have to articulate and elaborate those principles in internal policies, and to communicate them effectively throughout the organization. They also have to oversee the implementation of those principles through management decisions and actions. Bank Board members and senior executives are therefore one set of intended users of this document.

The design and implementation of a sound risk process is largely the responsibility of senior risk officers, business line managers, the dedicated risk management function as a whole, as well as other control functions within the bank, such as financial control and internal audit. Those constitute another set of intended users of this document.
I. KEY PRINCIPLES OF SOUND RISK GOVERNANCE

The principles described below are relevant to any banking institution, at almost any stage of development, and in any jurisdiction. Their practical implementations can vary, however, depending on regional and local factors and the institution’s size, nature, and complexity. Nevertheless, any banking institution should be able to understand the spirit of these principles and their practical implications for the bank’s activities. Every bank should strive to develop its own practical means of observing those principles, and should be able to demonstrate to outside reviewers both its actions in that direction and their effectiveness.

1. RISK APPETITE DETERMINATION

Financial institutions need to determine their appetite for different types and levels of risk, carefully taking into consideration their organizational capacity to manage such risks. The comprehensive understanding of that risk appetite throughout the various levels of an organization should drive the balancing of risk and return, the allocation of capital, product pricing, as well as incentives and remuneration structures for employees, management, and Board members. Business strategy as the backbone of revenue pursuits needs to be developed and continuously brought in line with that risk appetite.

1-A Some Background on the Fundamentals of Financial Risk and its Theory

Risk in financial theory is defined as potential loss from some aspect of financial activity. The concept of risk is clearly related to uncertainty, chance, predictions of future events with imperfect foresight, and developments outside of one’s control. Risk is one of the main subjects of statistics, an actively developed branch of economics, and an integral part of any social science.

The dichotomy of risk and return is a widely accepted tenet of finance. The relationship between the amount of risk inherent in a financial activity and the amount of loss or gain expected and ultimately resulting from that activity is often both intuitive and evident from careful observation.

Therefore, it should be obvious that, in the world of business and finance, the ability to control future revenues is at least in part dependent on ability to control exposure to risk. In particular, when a specific level of financial result is pursued (through business strategy and planning) then it should be understood that an exposure to a closely related level of risk will be taken. This generally means that if higher gains are sought, they are likely to be accompanied by exposure to greater risks (i.e., the possibility for greater losses).

Even if on average the high return/ high risk and the low return/ low risk strategies are expected to produce similar net results, the types of people, systems and processes required by those strategies are by necessity very different. Those differences apply to both the revenue generation side of the business and to the risk management and mitigation side of it.

Therefore, a bank’s management needs a good understanding of the tradeoffs between risk and return that result from different business strategies. It also needs to assess thoroughly which tradeoffs its institution is capable of taking – given its human and technological resources, knowledge base and position in the market. Without that understanding, pursuing any business strategy is at best uninformed, and often worse – irresponsible. Developing that understanding is the essence of risk appetite determination.

The risk appetite determination should be performed by the Board of Directors (the highest level of management) as an integral part of choosing a business strategy for the bank. The amount of risk the Board is willing to accept may be related not only to the desired level and certainty of profits but also to the pursuit of other business objectives, such as market share, innovation, recognition, etc. Ultimately, however, the tradeoff between risk and revenue (return) is the most useful and clear way to express risk appetite.

1-B Difficulties in Determining Risk Appetite

Although many bank executives and board members are familiar with the concept of risk appetite and would agree that a bank needs to
Standards on Risk Governance in Financial Institutions

determine its own risk appetite, the practical implementation of that is far from trivial. This is, in part, why a widespread reluctance exists to engage in this exercise.

Part of the difficulty relates to measuring how much of a gamble, or tradeoff, “is worth” making, to obtain a desired level of return - which is largely a subjective, psychological preference, and varies from one person to another. Risk appetite, alternatively expressed as risk aversion, is the willingness to take a certain gamble for a certain return.

Another difficulty is the measurement of risk itself. Risk appetite/ tolerance/ intolerance has to be expressed in terms of “how much risk” to take. However, the very measures of risk – although more objective and consistent, are far from perfect. They become particularly hard to use when comparing across different “types of risk” (e.g. market, credit, liquidity, operational) or when combining them to measure and compare complex activities. All of that makes it difficult, indeed, to express appetite for risk consistently and reliably.

Nevertheless, risk appetite is one of few variables that an organization can control – unlike market circumstances, regulation, and other external factors. Therefore it is a critical contributor to the success (or failure) of any organization.

The comprehensive understanding of risk appetite throughout the various levels of an organization affects directly the balancing of risk and return, which means the allocation of capital, product pricing, and employee incentive structures. Business strategy as the backbone of revenue pursuits needs to be developed and continuously brought in line with risk appetite. Strategic goals, objectives and incentives should be set in a way and at levels that can be attained while assuring sound operation and without exceeding the maximum risks the institution is willing to take.

It should be well understood that banking institutions are not completely free to set their own risk appetite. Regulators, concerned about systemic risk, impose constraints designed to prevent excessive risk taking in pursuit of higher profit. Therefore, regulatory rules, including capital adequacy and liquidity requirements, also set bounds on risk appetite.

Once set, the risk appetite level needs to be reassessed regularly – at least once a year, and more often if required - in view of changes in the business environment and as measures and understanding of risks evolve.

I-C Components of the Risk Appetite Determination Process

Risk-Return Tradeoff

The Board needs to show clear recognition that there is a tradeoff between risk and return – that is, that seeking higher levels of return would generally involve higher risk and the possibility for greater losses.

Interests of Various Stakeholders

The Board needs to give explicit consideration to the interests of various stakeholders (e.g., shareholders, lenders, depositors, customers, regulators, etc.), and to agree on order of priority wherever those interests diverge.

Individual Risk Preferences (Degree of Risk Aversion)

Board members need to articulate their own individual risk preferences and then be able to coordinate and agree on an institutional level of risk preference, suitable to the capabilities and the culture of the institution, its strategy and its business environment.

Risk Identification and Measurement Capabilities

A well-developed risk assessment system is required to allow the Board to identify different types of risk and obtain estimates of their levels associated with different business strategies. Where quantitative measures are impossible to obtain, clear and comprehensive qualitative descriptions of risk should be developed.

Translating Risk Tolerance into Metrics and Guidelines

To the extent that risk measurement capabilities permit, risk appetite needs to be expressed in terms of the standard risk measures used by the organization. This makes it easier to inform
decisions at lower levels in the organization and to “apportion” risk appetite in a coherent way between business lines, products, types of risks, etc. As risk metrics are bound to be lacking in some areas, however, appetite may also need to be described in qualitative terms.

Another useful way for the Board to achieve clarity in defining risk appetite is to consider, and describe in maximum detail, what risks specifically it will not accept, as well as what new risks it will seek through new business lines, products, market segments, etc. Appetite may also be expressed in terms of a range of acceptable outcomes / variation of results.

Other forms of expressing risk appetite include:

- setting a target credit rating
- setting a Value-at-Risk limit
- setting a target rate of return on equity, capital, assets, risk-adjusted assets, etc. (sometimes, but not always accompanied by a target limit on the variance of that return)
- determining a level of economic capital that the bank will maintain to cover the risks it takes, and approving an allocation/ cascading of that capital to risk categories and business lines in a manner consistent with the bank’s business strategy
- setting target levels for key risk indicators, as well as high-level limits for credit, market, liquidity, and other risks; this level of expressing risk appetite is performed at both the Board level and the executive level, gradually translating in a consistent manner the high-level risk appetite parameters defined by the Board into specific business activity parameters.

Where trade-offs and competing objectives are expected and can be identified, effort should be made to design and articulate broad principles that would guide preferences in all specific situations and would lead to consistent decisions across units, individuals, and over time.

Just as with risk measurement, in setting a risk appetite level, the institution has to take all relevant risks into account, including those arising from off-balance sheet transactions, contingent liabilities, remote geographic locations and legal entities.

Strategic objectives may include non-commercial components. This is especially relevant for banking institutions with a significant government ownership stake. Those social or other policy-related objectives need to be defined as clearly as possible, and - ideally – quantified. Thus, objectives such as stimulating economic growth, creating jobs, good citizenship, responsibility for the financial safety of customers, and the like, are best expressed in monetary terms, so that the associated risks, costs and trade-offs may be clearly taken into account when defining risk appetite and aligning it with strategy.

1-D Apportioning and Communicating Risk Appetite down throughout the Bank

After appetite is set at the highest aggregate level it needs to be apportioned and balanced at lower levels - for individual business lines and units, different products, geographies, as well as for different types of risk. This process, also called cascading, involves complex considerations of risk dependencies – correlations and offsets – that should be given full attention. Although in practice it is hard to achieve precision in this process, it should nevertheless be given maximum effort and the clearest possible definition.

1-E Communicating Risk Appetite Externally

The Board also has a responsibility to ensure that the bank clearly communicates its risk appetite outside the organization, to all stakeholders and other external parties that may be affected, such as investors, regulators, depositors, and the general public.

2. RISK-BASED INCENTIVES AND COMPENSATION

Financial institutions should remunerate and incentivize employees and management on the basis of long-term, risk-adjusted value added to the organization. Profitability of business units and any measures of financial returns should be adjusted to reflect measures of associated risks.
The issue of behavioral incentives affects risk governance at every level of the organization - from the Director or senior executive level that steers business activities in the direction of particular markets, products, customer segments and business practices, to the front office / sales and trading function that makes individual risk-taking decisions on behalf of the bank through every transaction. At all levels of the bank, excessive focus on short-term profit without regard to risk and longer-term financial impact has proven to be a fatal risk governance flaw.

As a guiding principle, employees and management should be remunerated on the basis of long-term, risk-adjusted value added to the organization. Their remuneration should also be adequate for the roles that they perform. In determining “adequacy”, the organization should reference not only supply and demand through external benchmarks, but also the anticipated financial contribution of the risk-taking/ revenue generation, or risk-mitigating/ revenue preservation function performed by the employee.

Excessive reliance on a variable pay component, including stock options, the value of which is linked to the short-term market price outlook for the company, is now widely considered destabilizing and is discouraged.

The remuneration of company directors and their performance evaluation has been found to be especially important for long-term institutional performance and viability. For this reason, in many developed economies there is regulatory action under way to publish director remuneration policies and individual salaries, and to establish some form of control, such as a vote, on director remuneration.

The impact of remuneration and incentives is less visible but equally important at the level of the control functions, including the risk function. There, the main problem is the lack of a widely accepted and transparent methodology of measuring those functions’ contributions to “the bottom line”. Notwithstanding this problem, giving appropriate incentives to control functions, including risk management, is absolutely necessary for ensuring that they perform their functions to the best of their ability and in the best interest of the institution.

3. CONFLICT OF INTEREST ELIMINATION

The avoidance of any form of conflict of interest is an absolute requirement of sound risk governance. A well-developed process of eliminating potential situations of conflict of interest should be in place for all new Board members, executives, and employees. Segregation of duties, independence of control functions from revenue generation functions, and proper checks and balances at all levels of the organization should be instituted and consistently maintained.

Closely related to the incentives that influence decision-makers is the issue of conflict of interest, or simultaneously holding mandates for different parties where the interests of one contradict the interests of the other.

Conflicting incentives arise often and affect every organization. In the financial services industry, especially in more recent years, the complexity of financial products and services, the volume of financial transactions, and the extensive links of financial institutions to all levels of the economy increase the difficulty of identifying and resolving such conflicts in a timely manner. This in turn increases the risks they pose, including reputational and legal risk to the institution itself, risks to investors, consumers, institutional clients and counterparties, as well as systemic risk.

Conflicts of interest are harmful to an institution even if there is no harmful intent, and even if no unethical or improper act results from them. The mere distraction of having to balance conflicting priorities can lead to suboptimal decisions. The mere appearance of impropriety can create reputational risk, undermine confidence in the institution, and bring about tangible negative consequences – e.g., withdrawal of funding, increase in borrowing costs, loss of customers, etc.

Some typical situations that give rise to conflict of interest in financial institutions include:

• representing both lender and borrower, e.g.
  when a board member of a financial institution
I. KEY PRINCIPLES OF SOUND RISK GOVERNANCE

also has business or personal connections to a large credit customer of that institution; or when a credit officer is reviewing a credit application from a related party

- using confidential client information to profit – e.g. when a financial institution makes investment decisions or provides investment advice to a third party on the basis of information that is not publicly available but was obtained in confidence from a client; or when an employee or officer transacts in the securities of such a company

- conflicting interests between a financial institution and its investors if they also have holdings in a competing business

- outside employment or other external affiliations with competitor organizations, vendors, or customers that have the potential to provide personal benefit to the officer or employee involved, while harming the institution

- political activities, affiliations and financial contributions related to external organizations that can pose reputational risk to the bank

- acceptance of gifts, gratuities and other compensation from parties that seek preferential treatment or stand to benefit in other ways at the expense of the bank

Some recent regulatory opinions also point to possible conflicts of interest between financial institutions’ creditors on one side (depositors, life insurance policy holders or beneficiaries of pension schemes and, to a certain extent, employees) - who are exclusively interested in long term viability, and – on the other side - shareholders, who are mostly focused on short term profitability.

The avoidance of any form of conflict of interest is an absolute requirement of sound risk governance. A well-developed process of assessment should be in place for new board members, executives, and employees, including standard disclosures and signed statements of compliance. Thorough periodic reviews and updates are also necessary to prevent or neutralize new situations creating conflict of interest. A procedure needs to exist for dealing with such a situation and no compromise can be made when it is discovered - the person involved should be relieved of all duties, at least until the conflict is resolved. Appropriate codes of ethics, arm’s length and related party transaction rules should be carefully developed and vigorously enforced.

3-A Independence, Segregation of Duties

Preventing conflict of interest is achieved through putting in place key checks and balances. Perhaps the single most important one of those is the separation of any risk-taking decision from the risk assessment and controls over it, i.e., making those functions independent. The main vehicle for implementing the independence principle is organizational structuring at all levels.

The segregation of Front Office from Back Office functions is a fundamental requirement of risk governance. Proper segregation means that the Back Office not only performs support functions that increase the efficiency of the organization but it also exercises control functions that impose discipline and reduce operational risks due to fraud and human error. (It should be noted that appropriate IT systems can serve to replace Back Office staff in both functions.) Proper segregation also means that reporting lines for all Back Office staff lead up to a senior level executive independent of any business origination/ Front Office function. Although now ubiquitous, or at least strongly embedded in financial services organizations domiciled in mature markets, this line of segregation may not be fully in place in developing markets and very small or young organizations – which is acceptable up to a point on the basis of cost considerations. This segregation is, however an imperative step towards establishing proper risk governance.

The Risk Management function, just like Audit, Finance, the Back Office, and other control functions, needs to have an independent reporting line directly through to senior management – preferably to the CEO, and in any case not through any business line that it is responsible to control. The head of the risk management function (CRO or equivalent) should have, ideally, a direct reporting line to the CEO and direct access to the Board. A CRO who reports to the head of
a business line is not free to effectively exercise control over the activities of that business line. A CRO reporting through Finance (i.e. to the CFO) does not have sufficient leverage to push through complex or uncomfortable risk issues to the highest levels of decision-making. 

The existence of the independent risk function also means that for all risk-taking activities there are multiple levels of risk assessment - one at the point of the risk-taking function, one at the point of the independent risk function, and a third “line of defense” - at the point of the independent audit review. Those multiple views of risk not only act as an operational safety measure, safeguarding against conflict of interest, human error, imperfect information, or outright fraud, but they also contribute to increased transparency and improved communication.

3-B External Validation

As an extension of the Conflict of Interest and Independence principles, an independent layer of controls that is external to the institution is also required for sound risk governance. This

---

1 It should be noted that multiple functions bearing the name “risk management” may exist in larger organizations. Some of those may be part of the front office and in fact be engaging in risk-taking activities, with specific responsibility for their quantitative analysis and risk assessment. Those “front office risk management” units are different from the risk management function described here and routinely referred to as the “dedicated risk management function” (or the “independent risk management function”).
I. KEY PRINCIPLES OF SOUND RISK GOVERNANCE

is most commonly performed through the engagement of external auditors. Rating agencies also perform a function of independent external evaluation. Independent external validation of asset valuations and other information used in reporting financial results is another direct extension of the independence principle and has been made a requirement by many regulators.

All aspects of the governance framework of the organization should be periodically validated by an independent body or bodies external to the organization. This will counteract any inherent conflicts of interest and will ensure that risk governance is in line with the markets, sectors, geographies, and other external factors in which the organization operates. It will also contribute to consistency between internal policies and public representations made by the organization.

4. PERVASIVE RISK CULTURE

Financial institutions must continuously develop a culture of understanding risk, recognizing the importance of risk management, and carrying personal responsibility and accountability for identifying and managing risks.

Beyond setting the right policies and structure, risk culture plays a major role for the success of an organization in its risk management. Building a risk-aware culture requires recognition -- at all levels and by all members of an organization -- of individual responsibility and accountability in identifying and managing risks. It also requires continuous feedback and realignment of business objectives, assessment processes, and employee incentives. This is a long and arduous process but its impact is long-lasting and far-reaching.

As with setting risk appetite and performing formal risk assessment, the risk culture must also extend across all of the organization’s units and business lines and encompass all relevant risks, both financial and non-financial (e.g. reputational risk).

4-A Accountability, Disclosure, Transparency

Putting a sound organizational structure in place, with strict independence and removal of all conflicts of interest, at all levels of the organization, does not remove the need for defining clear accountabilities. Board members, executives, departments and individual staff members should be clearly advised of their own accountabilities and of the consequences of not fulfilling them in a timely and appropriate manner.

Disclosure and transparency create the best environment for accountability. They need to be fostered through formal requirements, as well as through the more informal daily interactions within the organization and between the organization and its external stakeholders – investors, customers, regulators and business partners. The Board of Directors and senior management need to promote an approach of disclosure and transparency by setting an example, in stated policies and through every other channel of communication.

4-B High Ethical Standards

Even the most extensive efforts to regulate, to mandate principles and to set specific rules, cannot exhaustively cover the situations and required behaviors that would guarantee sound risk governance. Honesty, trustworthiness, fairness and concern for the interests of others would still need to be invoked in situations where other principles are insufficient. The key people involved in the application of good governance and risk management must also set the highest ethical standards of behavior.

4-C Important Risk Awareness Behaviors

A positive risk culture is expressed in a number of routine behaviors:

- Employees across the organization are aware of risks and proactively take risk considerations in mind in their everyday work
- There is respect and appreciation for the role of the dedicated risk function, willingness to support its activities, to understand its output, and to learn from it
- There is openness and willingness to disclose and discuss information related to risks, and to challenge established views and assumptions
- All levels of the organization feel responsible for and adhere to the principles of sound risk
Standards on Risk Governance in Financial Institutions

governance in a collaboration that fosters not only top-down oversight but also bottom-up involvement from front-line risk takers.

• The risk function views itself and is viewed as supporting and contributing to business success, instead of only as imposing control and restraint

• Risk measures and methodologies are consistent and well-integrated across businesses and risk types

• There is good coordination between the Risk and Finance functions as part of a proper risk-adjusted profitability framework for business planning and incentive structuring

• There is a good balance between quantitative and qualitative assessment of risk - employees strive for quantitative sophistication - however, they understand its limitations, including assumptions, data availability and systems capability

5. EFFECTIVE COMMUNICATION

Sound risk governance requires highly effective communication that includes educating, collecting feedback, reporting, and engaging in constructive dialogue about risk. Communication of risks is just as important for sound risk governance as measuring and controlling them. The role of risk managers and of everyone involved in the risk process should include a significant responsibility for communicating risk information throughout the organization.

Effective communication of risk issues is, in many ways, another element of a pervasive risk culture. However, it affects so many aspects of the risk process in very specific, sometimes formal, ways that it is useful to address it as a stand-alone principle.

Communication includes educating, collecting feedback, reporting, and engaging in constructive dialogue about risk. Communication of risks is just as important for sound risk governance as measuring and controlling them. The role of the risk manager and of everyone involved in the risk process should include a significant responsibility for communicating risk information throughout the organization.

Effective risk governance requires an ongoing discussion that produces consistent views:

• between the board (which sets risk appetite and oversees), senior managers and business unit heads (who execute), and risk management (who design and perform risk measurement)

• between front office and risk management staff

• between the various control functions

• within the risk management organization – among subunits, hierarchy levels, and among individual staff members

• A variety of methods and tools should be employed to communicate risk, including:

• Narratives and charts of business objectives linked to risk tolerance levels

• Dashboards and detailed reports of key risk indicators, limits, and suggested actions, with visual status of where key risks stand relative to risk tolerances

• Flowcharts and maps of processes with key controls

• Discussions and briefings on routine and special topics

6. STRONG CHIEF RISK OFFICER AND RISK FUNCTION

Every financial institution should have a designated senior executive responsible for all aspects of risk management and all types of risk – typically called the CRO. The organizational hierarchy and the allocation of executive powers should reflect the CRO’s and the risk function’s importance as being on par with those of revenue-generating functions.

The risk management function in every organization should be given adequate status, authority and resources.
The characteristics of a strong CRO include:

- independence from any business line
- membership in the Executive / Management Board allowing direct influence on strategy setting
- the ability to challenge and potentially veto risk-related decisions of the Management Board
- a direct reporting line to the CEO; some recent research points to a direct reporting line to the Supervisory Board as an even stronger position, with measurable advantages
- financial compensation commensurate with that level of importance in the organization

A strong risk function also involves a dedicated board-level risk committee. It is now widely believed that a majority of independent directors on that committee strengthens its contribution to risk governance. Another factor that strengthens the risk function is a high percentage of committee members with strong financial expertise and background, as is a regular schedule of committee meetings and discussions.

Finally, the financial and technological resources available to the risk function are also a measure of risk function strength and should be commensurate with the complexity and importance of its role.

7. STRONG RISK COMPETENCIES

Financial institutions should hire and continuously train a sufficient number of risk management professionals who have adequate business experience, are highly competent communicators, and are proficient in all aspects of risk theory, including economics, financial theory, mathematics and statistics, information science, and information technology.

The organization should develop a thorough understanding of the knowledge, skills and expertise required of those involved in risk management to perform their roles successfully. Those competencies should be clearly described and systematically assessed in the hiring process, including through formal testing or certification requirements. In general, all risk management staff would be expected to exhibit high competency in economics, financial theory, mathematics and statistics, as well as significant IT proficiency. Many risk managers would also need to demonstrate superb verbal and written communication skills.

Requirements should not be limited to formal education but should include, in most cases, a practical business experience component.

When skills or experience are not readily available from the regular job applicant pool, specialized training should be organized to compensate for lacking elements. As much as possible, experience in risk management roles should be supplemented with experience in other roles and units. It is especially useful to provide risk managers with knowledge and experience of risk-taking roles, and of products, customers and markets for which they will be performing independent risk oversight.

Conversely, ongoing risk training should be provided to front office staff, and rotations into risk assessment roles should be organized as much as possible to increase their risk competencies.

Risk management is a dynamic and complex discipline, and banking is an industry conducive to rapid product development and innovation. For both of those reasons those involved in risk management should continually upgrade their skills and experience. The institution should organize group training initiatives and should encourage and financially support employees’ individual efforts to keep abreast of developments in their areas of expertise through courses, conferences, journals, memberships, and other channels.
II. ORGANIZATIONAL STRUCTURE and KEY PARTICIPANTS

This section describes the traditionally established management bodies and individual roles within a banking organization that carry risk management responsibilities and contribute to sound risk governance.

The governance and organizational structures of banks are at least in part dictated by specific national laws and regulations, which accounts for national and regional variations. The opening up of national economies and globalization of capital markets, however, has facilitated a gradual process of harmonization of regulatory regimes that has now been in motion for over two decades. Therefore corporate governance in general, and risk governance in particular, is carried out through broadly similar structures in a large variety of banking organizations and geographies.

1. THE BOARD

The Board of Directors acts on behalf of shareholders to set policy, strategy and objectives, and to oversee the executive function. It sets risk appetite and ensures that it is reflected in business strategy and cascaded throughout the organization. It establishes and oversees an effective governance
and organization structure in accordance with legal, regulatory and fiduciary responsibilities that would allow it to put in place effective risk governance.

**1-A Composition and Selection**

The composition of the Board and the process of board member selection are two of the most important factors for ensuring the quality of the Board’s work. There are several key criteria to be observed:

**1-A-1 Competencies**

- The Board needs a sufficient number of members with deep understanding of finance and risk that allows them to critically assess and challenge opinions and proposals presented to them by the Executive.
  
- Board members’ financial expertise should cover not only issues within the organization but also outside of it – i.e., they should be able to assess the business environment and be comfortable with subject matter related to macroeconomics, financial markets, and the financial system as a whole.

- Appropriate training and development should ensure that the Board’s qualifications remain adequate through periods of business expansions, business model and strategy changes, and changes in the external environment.

- All Directors should also be familiar with the organizational structure of their financial institution and be able to make decisions that account for its characteristics.

**1-A-2 Independence**

- Conflict of interest can be particularly harmful at the Board level and therefore all possible measures should be taken to prevent it.

- A Supervisory Board should be composed predominantly of non-executive directors.

- Outside affiliations should be carefully examined and conflicting interests eliminated before Directors can carry out their governance responsibilities.

**1-A-3 Diversity**

- Deep expertise in finance and risk should be supplemented with other competencies and characteristics; non-financial aspects of business management should also be covered among the combined Board competencies.

- It is also believed that representation of different social, cultural and educational backgrounds among directors can contribute to a more complete understanding of the different environments in which the bank operates.

**1-B Clear Mandate and Accountability**

- Each Board member should have a clear understanding of their role in corporate governance and should be held accountable for performing it.

- Board members’ obligations, including time and other resource commitments should be explicitly defined.

- Board members’ performance should be routinely and formally evaluated, and it should be subject to a well-defined incentive and penalty system.

**2. BOARD RISK COMMITTEE**

The Board may choose to perform its risk oversight responsibilities through a dedicated group of its members, the Board Risk Committee (sometimes called Risk Policy Committee). In smaller organizations a Committee may not be feasible but there should be at least one designated Board member responsible for risk issues.

In particular, the Committee is responsible, on behalf of the Board, for:

- making recommendations regarding Risk Appetite

- reviewing periodically the organization’s Risk Profile
• reviewing strategic decisions, such as acquisitions and disposals, as well as entry into new products and markets, from a risk perspective
• reviewing periodically the risk management and internal controls framework relative to the risk profile
• approving risk policies, limits and delegations
• considering any key risk issues brought by Management, or requesting information about risk issues that the Committee identifies independently
• reviewing and recommending for Board approval key policy statements required by regulators, such as those on concentration and large exposures, liquidity, credit impairment and provisioning, etc.

The Risk Committee possesses and continually develops risk expertise and devotes the necessary time to study risk issues and communicate extensively with the risk management function of the institution. It informs the Board, guides the process of risk appetite setting, and ensures that risk issues are given sufficient weight in the Board’s deliberations.

The Risk Committee makes sure that reporting is adequate to properly inform Board decisions, and that decisions are properly communicated and understood at the executive level. In addition, the Risk Committee ensures, through adequate oversight of the executive risk management function, that key external users of risk information, such as regulators, investors, auditors, and rating agencies, are given a complete picture and adequate interpretation of the risk profile of the bank.

The CRO should have direct access to the Board Risk Committee, both to present information and to raise issues.

A Risk Committee is also often set up at Management level – normally below the CEO. At that level the Risk Committee is usually chaired by the Chief Risk Officer (CRO) and assumes overall responsibility for implementation and adherence to the Board-approved risk management policies and standards.

3. BOARD AUDIT COMMITTEE

The Audit Committee’s typical responsibilities are the oversight of financial reporting and disclosure, as well as monitoring the effectiveness of the internal control process and of the internal audit function. Audit Committees also get involved in issues of regulatory compliance and dealings with external auditors. In the absence of a Risk Committee, the Audit Committee often steers most of the risk oversight functions of the Board. Through its direct access to the Board and through its oversight of the Independent Audit function (the “third line of defense”), the Board Audit Committee plays a critical role in the risk governance framework.

4. CHIEF EXECUTIVE OFFICER

The CEO of a banking organization must carefully balance the functions of revenue generation and risk mitigation. While every function below the CEO will inherently focus more on one of those objectives, the CEO and the Board need to find the right balance between them.

In their risk governance role CEOs are responsible for ensuring that all business is carried out with due consideration of the risk appetite set at Board level and that all risks are properly evaluated and managed. The CEO, together with the Board, bears the greatest responsibility for setting standards of behavior and influencing the risk culture of the organization.

5. CHIEF RISK OFFICER

Every bank needs to have a designated executive with broad and exclusive responsibility for all risk issues. That executive is usually called a Chief Risk Officer (CRO). The CRO performs the most critical executive function related to risk management. Best practice requires that the CRO is a member of the Bank’s Executive/Management Board, reporting to the Chief Executive Officer and possibly to the Board of Directors, through
II. ORGANIZATIONAL STRUCTURE and KEY PARTICIPANTS

The Board Risk Committee, when there is one. Additionally:

- The CRO should be actively involved, at an early stage, in the elaboration of the institution’s risk appetite and business strategy.
- The CRO should be able to adequately communicate their risk assessment to the Board and to facilitate sound Board-level risk decisions.
- The CRO should have sufficient technical expertise to properly understand the intricacies of an institution’s risk exposures.

6. CREDIT COMMITTEE

The Credit Committee (or multiple committees) is an executive body often set up directly under the Executive (Management) Board to perform active oversight and take responsibility for significant lending and other credit-related decisions – i.e., for credit risk. The CRO or Head of Credit Risk should play a significant role in those committees, but they are also a mechanism for bringing expertise and perspectives from other functions, including business lines.

7. ASSET AND LIABILITY COMMITTEE (ALCO)

Like Credit Committees the Asset and Liability Committee is an additional, specialized decision-making body that allows broader inputs from departments outside the dedicated risk function, such as Treasury, Finance, and Dealing/Money Markets to be included in the management of specific risks – particularly Interest Rate, Currency and Liquidity risks. ALCO is also usually set up at the executive level, below the CEO, and should actively involve the CRO or a high-level representative from Risk Management.

8. THE DEDICATED RISK FUNCTION

Below the CRO, a well thought-out structure of risk management functions and units needs to be established. It should be comprehensive - covering all risk types and business lines, and independent - under the direct responsibility of the Chief Risk Officer (CRO) who reports directly to the CEO or the Board.

Specifically, the Risk function should include units responsible for credit risk, market risk, liquidity risk, operational risk, and others (in larger and more diversified institutions). Further functional specialization should be done as necessary to create units for methodology, reporting, risk policy and risk technology.

The dedicated Risk function plays a key role in identifying, assessing, and managing the overall risks faced by the institution. The risk function should be staffed with sufficient and relevant technical expertise, a good understanding not only of risk concepts but also of the products and markets monitored, and provided with adequate technological resources.

Main Responsibilities

- The dedicated Risk function bears primary responsibility, together with the relevant risk-originating departments, for assessment and control of Credit, Market, Liquidity and Operational Risks
- Collects and analyzes information needed for risk assessment:
  - sourced from internal Bank systems, databases and reports, Back Office/Operations, Finance, Audit and other departments
  - from external sources - organizations and publications providing market data, forecasts and analysis
  - supplementary deal and market information, analysis and planning supplied by risk-taking departments
- Researches and implements external or internally developed risk measurement methodologies, including rating systems
- Estimates risk levels with its available methodologies
9. CHIEF FINANCIAL OFFICER

Traditionally, the CFO oversees all aspects of financial accounting, planning and management of the Bank. Historically, the CFO has often been responsible for the Risk function. Although more recently this has been changing to carve out the role of the CRO and elevate its status to that of the CFO, a large responsibility for Risk still rests with the CFO and the Finance function. Through analytical efforts, CFO's and the Finance function generate business insights that can help the Bank better understand the drivers of its performance, predict changes in performance, and react faster and more appropriately to changes in the business environment.

10. INTERNAL AUDIT

Internal Audit reports independently to the audit committee. It maintains appropriate measures to ensure that the Governance and Risk Framework of the organization is effective and all departments are in compliance with that Framework and with their internal policies and procedures. It conducts planned and ad-hoc investigations, escalates any shortcomings discovered, and recommends remedial action to be taken in an appropriate and timely manner. It prepares risk assessment and internal audit plans, executes those plans, tracks the implementation of all internal audit recommendations and external audit management points, and reports to the Board on their status and progress. Internal Audit is considered the “third line of defense” in the generally accepted risk governance framework.

11. LEGAL and COMPLIANCE FUNCTIONS

The Legal and Compliance functions ensure that the organization as whole, and each individual employee, understand the external rules and regulations with which they must comply and the implications of non-compliance. Those functions have to be particularly proactive in large, complex banking organizations that offer a wide array of products and/or products of high complexity. In those environments there is a higher risk of overlooking or failing to understand legal and regulatory requirements.
12. EXECUTIVE OFFICERS, INDIVIDUAL BUSINESS UNITS, ALL STAFF

The management of risks is not confined to the dedicated risk management function. It should be made an explicit responsibility of all senior management and of all staff in all business lines.

Every bank’s risk governance structure should be founded on the responsibility of each line of business to manage its own risks. They are responsible for providing the “first line of defense” in the risk governance framework. They work closely with the “second line of defense” – the dedicated Risk Management function - to make both transactional decisions and higher-level decisions regarding risk strategy, policies and controls.

Risk awareness and an appropriate level of risk training should be provided to all employees, compatible with their functions and levels of responsibility.
III. THE RISK MANAGEMENT PROCESS

1. OVERVIEW

There are several important goals of the risk management process (see Diagram below):

- to forecast potential losses, to assess whether to take, transfer, mitigate or eliminate them, and to propose ways of doing that
- to ensure institutional survival in periods of stress by ensuring that the institution holds sufficient capital to cover unexpected losses arising in the course of business and sufficient liquidity to meet its contractual obligations
- to help direct capital and incentives to the most profitable activities, products, organizational units and staff after their profitability is assessed on a long-term, risk-adjusted basis

To achieve those goals, the risk management process goes continuously through a cycle of identification, assessment, mitigation/control, and monitoring/reporting/evaluation of all risks.

2. IDENTIFICATION

Identification is the first step in the risk management process. It is a discovery and categorization exercise performed at every organizational level to look for all sources and types of risk arising from every product and service. Although it is a seemingly simple step, it requires rigorous analysis to avoid common pitfalls:

a) Risks can be “hidden” by accounting standards (e.g., accrual accounting can mask interest rate risk in the banking book)

b) Risks can also be hidden by the need to summarize information in reporting (thus basis risk is easy to miss when exposures to two closely related markets are netted out)

c) Risks can be contingent on other risks - e.g., liquidity risk can arise as a consequence of credit risk (from non-performing loans)

d) Risks can be ignored because historically they have been hard to quantify and/or they’ve been part of doing business without
III. THE RISK MANAGEMENT PROCESS

being measured or managed (e.g. this often happens with prepayment, early withdrawal, or contingent liability risks that are traditionally embedded in many banking products).

3. ASSESSMENT / MEASUREMENT

Quantitative analysis (measurement) of risks is one of the most complex and resource-intensive activities in risk management. Significant methodological and technological advances in the past few decades have enabled rapid development not only in financial products and markets, but also in risk measurement and management techniques. Sophisticated models and IT systems have helped to improve the scope and precision of potential loss forecasts through data-driven models, enabling forward-looking risk assessment and accounting for risk correlations and dependencies.

The ultimate objective in risk measurement - potential loss forecasts, expressed in terms of magnitude and in terms of likelihood - has become possible. Obtaining those kinds of measures with speed and precision, for all types of risks, products, and markets, however, remains not always possible and sometimes not practicable. Simpler, less precise or comprehensive measures still need to be used extensively.

3-A Exposures

By itself, exposure does not provide a loss forecast but is one component in its estimation. It is often used in practice as a substitute for a risk measure. In most situations, it is the component of risk that is easiest to quantify and so it often serves as an intuitive proxy measure of risk. It is useful to define exposures relative to a specific risk factor (or a category of risks, or a subset of them). For example, currency risk assessment is often done simply on the basis of a net currency open position - the exposure. The risk factor is an exchange rate or multiple exchange rates when multiple currency positions are involved. Additional risk factors are the correlations among those exchange rates. Concentrations are also effectively exposure measures, as interest rate or liquidity gap measures are. The usefulness of exposure measures can be increased by supplementing them with measures of the volatility or direction of trends in the risk factors that affect them. Thus, high concentration of the credit portfolio in the construction sector, shown alongside a negative trend in loan performance in that sector is a highly meaningful and actionable risk statement. This takes the risk analysis a step closer to probabilistic measurement and loss forecasting.

3-B Sensitivities

Sensitivity measures are important where computation of potential loss due to a given risk factor is well understood but technically involved and not intuitive. Two common areas of use are interest rate risk (sensitivity to interest rate changes – such as duration and convexity measures), and optionality risk (sensitivity to the underlying price (delta), to time (theta), and to price volatility (vega)). Sensitivity assessment centers on the impact of one risk factor. When the simultaneous impact of several risk factors is analyzed, then the process is usually called scenario analysis.

3-C Probabilistic Measures

Probabilistic measures, usually referred to as Value-at-Risk (VaR, or some variation of that) represent a statistical estimate of potential loss, given a chosen time horizon and confidence level. Probabilistic measures are the most ambitious and sophisticated type of risk measures, and the most versatile – provided they can be computed, and when they are properly understood. Their computation, however, requires data that is often unavailable, advanced models, theoretical assumptions, and – often - high-powered systems that may be unaffordable. Besides being “high-cost” due to those factors, probabilistic measures may also be hard to understand, which limits their usefulness to senior decision-makers who may have limited technical expertise.

3-D Scenario Analysis / Stress Testing

Stress testing is an exercise of explicitly assessing the potential impact of big shocks to risk factors (rates, prices, etc.) on portfolio returns and exposures. The results of stress testing are not usually tied to any measure of probability. They are thus arbitrary, or entirely dependent on assumptions about the severity and duration of the shocks to underlying risk factors. Stress scenarios
can be built using relevant market data from past extreme events (historical scenarios) or trends and expert forecasts of future risk factor movements (hypothetical scenarios).

3-E Risk Models

Models should treat risk in an integrated way, taking account, as much as possible, of correlations and interdependencies. Results should be compared routinely between different risk methodologies or models. Models should be tested, validated and calibrated on an ongoing basis. Assumptions, practical and conceptual limitations of metrics and models should be clearly identified, discussed at an appropriate level, and regularly revisited.

Quantitative models should be only one part of risk management assessment. Qualitative descriptions and expert judgment remain an important part of risk management. However advanced the state of the art in measurement may be, the possibility for complete and precise measurement of all risks, i.e., complete reliance on quantitative methods, is not yet in sight – even for the most sophisticated banks. The need to make assumptions, the complexity of economic events and their impact on financial variables, the inability to observe relevant factors and collect some of the necessary data makes quantitative approaches insufficient. Where they cannot be used or their output is not reliable, it is necessary to resort to qualitative and/or subjective evaluation.

3-F Additional Considerations

3-F-1 Critical Non-quantitative Factors of Assessment

It should be emphasized that successful risk assessment, especially in traditional banks, is less dependent on technological sophistication and much more dependent on understanding of assumptions and limitations of measures, and the interpretation and communication of risks with great consistency and discipline. Moreover, simpler risk measures can often be more useful if they are more easily explained and more intuitive. Advancement of risk measurement IT systems and methodologies should be a standing objective for every bank but that in itself does not guarantee good risk management. Thorough understanding of risk factors, of the meaning of risk estimates and their limitations, and of assumptions used in the estimation, is much more likely to produce good risk management decisions.

3-F-2 Cost-Benefit Considerations for Risk Assessment

The quality of risk assessment depends to a great extent on the quality and size of the human and technological resources dedicated to it. It is reasonable and necessary to consider the cost of risk assessment at various degrees of sophistication, against the potential benefit in terms of value preserved. Thus, if taking on a certain type of risk through a specific product or type of customer is too costly to properly measure and understand, this should be weighed explicitly against the anticipated revenue from that activity. Ultimately it may be decided to forego that particular business opportunity due to the high cost of risk assessment.

4. CONTROL / MITIGATION

4-A Limits and Other Mechanisms

A well-designed limit system is one of the key mechanisms for risk control and mitigation. Limits can be set on the various risk measures, including exposures, sensitivities, statistical risk measures, or actual losses.

Other risk control and mitigation mechanisms may involve risk-based pricing, loss provisioning, collateral and other credit enhancement requirements, and hedging strategies.

Risk mitigation can be initiated by business units or by the Risk Management function. The latter either participates in, or has primary responsibility for developing relevant methodologies. The execution of risk mitigation activities is typically the responsibility of business units.

4-B New Product Approval

For both new and established institutions, development and launching of new products presents a special risk management challenge. Best
practice dictates that a “new product approval process” (NPAP) should be in place, that covers not only entirely new products, but also significant changes in the features of existing products, significant differences in new market segments where existing products are to be offered, as well as any new processes that have risk implications. Responsibility for managing the NPAP should be vested in a dedicated function, which is often part of Operational Risk.

5. MONITORING / REPORTING / COMMUNICATION/ EVALUATION

Sound monitoring and reporting systems allow effective prioritization and escalation of the most relevant information to the appropriate decision-makers and other users in the bank. In designing the reporting system, proper attention should be given to several factors:

- content of reports (coverage, metrics, visualization tools, supporting information and interpretation)
- presentation (a balance of numbers, graphics, and text)
- frequency of production
- audience/distribution
- means/medium of presentation

Evaluation of the effectiveness of the risk process should be carried out consistently in the course of monitoring and reporting. It should provide feedback to continuously update and improve all preceding steps in the process.
CONCLUSION

To achieve success and gain recognition for sound risk governance and risk process, banks need to maintain focus on two types of priorities. One is the continuous and exhaustive coverage of fundamental requirements and the exercise of established and familiar measures of control, without fail. The other one is the need for swift, bold measures to anticipate and deal with the newest, most pressing issues of the market.

In terms of risk governance, the current pressing issues in the banking industry worldwide center on the role, competencies and incentives of Boards and senior executives, on removing conflicts of interest at all levels and raising standards of accountability.

In terms of risk process, those issues include the need for higher capital buffers that are less prone to the effects of the business cycle, a more conservative definition of capital, a more thorough liquidity adequacy framework, better designed stress testing, more adequate valuations, more serious attention to counterparty credit risk, and sharp curtailment of leverage. In one way or another, through the interconnectedness of the global financial system, these are issues that have real potential to affect banks of all sizes, at all stages of development and in all geographies.

The presentation of these Standards is broadly consistent with the latest guidance produced by international and national consultative bodies, regulators, scholars, and professional associations.

Some issues of great regulatory concern that have not been addressed here include the use of high leverage through derivatives and other complex financial instruments, and the role of complex and opaque legal structures. Those types of issues relate primarily to highly developed financial markets. However, they should be kept in sight as local market players become more active internationally and the local market’s level of complexity continues to increase rapidly.

There is another category of issues that have received intensive public attention in recent years and deserve mention here, although remaining outside the scope of this document. They include the ineffective implementation of governance standards - despite the existence of extensive standards - and issues related to the role of shareholders, supervisory authorities, and external auditors. Those issues are just as relevant to emerging markets as they are to mature markets. However, their causes and manifestations are different and they are not as extensively studied and analyzed in the context of emerging markets. We set them aside for the moment, noting that they should be examined as soon as possible.

Through the improvement of individual banking organizations risk governance standards also serve as a tool for mitigating systemic risk, which has been at the forefront of regulatory attention ever since the global financial crisis began to unfold in 2007.

The sound risk governance of banking institutions is of paramount importance not only in large economies and developed financial markets. The banking system plays a central role in an economy of any size. Moreover, financial institutions around the world are so highly interconnected now, within and across national borders that the failure of one bank to meet its commitments could set off a chain reaction of problems and failures in the global financial system, as recent examples have shown. Large numbers of individuals and institutions can be affected – including customers, counterparties, creditors, shareholders and other stakeholders, far beyond the country and the region of the problem institution.

A banking crisis can quickly transmit its ill effects to the real economy through the contraction of credit and other mechanisms, as recent and more distant history has shown. This transmission is at the heart of systemic risk.

Understanding the principles of risk governance and the framework of risk is an indispensable requirement for any financial institution. Without such understanding it is impossible to deal effectively with either the ongoing requirements of risk management or the pressing risk issues of the day.
Appendices
Appendix 1: Evaluation Table – Key Risk Governance Principles

The following table is used for shortcomings identification, tracking progress, and planning activities in strengthening risk governance in the Financial Institutions. Evaluation criteria are applicable to any types of financial institutions and scale of activities. However, benchmarking criteria may vary on risk the financial institution is exposed: the more institution is risk exposed the more level of risk governance it should meet.

<table>
<thead>
<tr>
<th>Evaluation Criteria</th>
<th>Benchmarking Criteria</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Unsatisfactory</td>
</tr>
<tr>
<td>1 Risk Appetite</td>
<td></td>
</tr>
<tr>
<td>1.1 Form of discussion on Risk Appetite in the Board</td>
<td>Not at all</td>
</tr>
<tr>
<td>1.2 Frequency of discussion on Risk Appetite in the Board</td>
<td>Never</td>
</tr>
<tr>
<td>1.3 Risk Appetite measures</td>
<td>Not measured</td>
</tr>
<tr>
<td>1.4 Top-down communication on Risk Appetite</td>
<td>Not at all</td>
</tr>
<tr>
<td>2 Risk-Based Performance Measurement and Incentives</td>
<td></td>
</tr>
<tr>
<td>2.1 Risk consideration in business unit profitability measurement</td>
<td>No</td>
</tr>
<tr>
<td>2.2 Risk consideration in staff performance evaluation and remuneration structure</td>
<td>No</td>
</tr>
</tbody>
</table>
# Appendix 1: Evaluation Table – Key Risk Governance Principles

<table>
<thead>
<tr>
<th>Evaluation Criteria</th>
<th>Unsatisfactory</th>
<th>Base Level</th>
<th>Improved Level</th>
<th>Advanced Level</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>2.3 Risk consideration in management performance evaluation and remuneration structure</strong></td>
<td>No</td>
<td>Risk taken into consideration but informally/ inconsistently</td>
<td>Risk formally mentioned among performance criteria</td>
<td>Risk formally mentioned and measures of risk specified in performance criteria</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>3 Conflicts of Interest (CoI)</strong></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>3.1 External/ independent directors on the Board</strong></td>
<td>No independent directors, independence not a requirement</td>
<td>Some independent directors; no formal requirement for their number or % of Board</td>
<td>Many directors independent; there is a formal requirement for a number or % of independent directors on the Board</td>
<td>Strict independence requirements stipulated, majority of Directors including most Committee chairs are independent</td>
</tr>
<tr>
<td><strong>3.2 Conflict of Interest avoidance and resolution</strong></td>
<td>No CoI avoidance measures in place</td>
<td>Some consideration given to CoI; there is awareness of the issue and informal checking takes place</td>
<td>Board members and management appointed only after meeting formal CoI requirements /&quot;test&quot;; Self-reporting of conflict of interest situations mandated for all; actions mandated to remove CoI situations immediately</td>
<td>Formal CoI process includes all actions from previous level and a routine for ongoing surveillance</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>4 Independence, Segregation of Responsibilities</strong></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>4.1 Front Office separate from Back Office</strong></td>
<td>No, same staff performing both functions;</td>
<td>Some segregation of duties exists but is inconsistent and one manager oversees both</td>
<td>Clear segregation of duties with different management/ reporting lines</td>
<td>Clear segregation of duties with different reporting lines through to different senior level executives, clear understanding of necessary controls</td>
</tr>
<tr>
<td><strong>4.2 Internal Audit function independent of business</strong></td>
<td>Independence is questionable</td>
<td>Segregation of duties exists but reporting lines converge too quickly (to one manager at some level below CEO)</td>
<td>Staff and reporting lines completely independent</td>
<td>Clear segregation of duties with different reporting lines through to different senior level executives, clear understanding of necessary controls</td>
</tr>
<tr>
<td><strong>4.3 Finance function independent of business lines</strong></td>
<td>Independence is questionable</td>
<td>Some segregation of duties exists but is inconsistent and one manager oversees both</td>
<td>Clear segregation of duties with different management/ reporting lines</td>
<td>Clear segregation of duties with different reporting lines through to different senior level executives, clear understanding of necessary controls</td>
</tr>
<tr>
<td>Evaluation Criteria</td>
<td>Unsatisfactory</td>
<td>Base Level</td>
<td>Improved Level</td>
<td>Advanced Level</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>-------------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>4.4 Credit Risk function independent of</td>
<td>No, front office bankers perform credit analysis and underwriting functions</td>
<td>Underwriting decision is technically independent (e.g. a credit committee) but analysis performed and recommendations given by front office</td>
<td>Dedicated staff and management for credit analysis, underwriting and monitoring; however, reporting lines lead to the same senior level executive below the CEO</td>
<td>Clear segregation of duties with different reporting lines through to different senior level executives; clear understanding of necessary controls</td>
</tr>
<tr>
<td>business lines</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.5 Market Risk function's independence</td>
<td>Independence is questionable</td>
<td>Some segregation of duties exists but is inconsistent and one manager oversees both</td>
<td>Staff and reporting lines independent</td>
<td>Clear segregation of duties with different reporting lines through to different senior level executives; clear understanding of necessary controls</td>
</tr>
<tr>
<td>4.6 Other Risk functions’ independence</td>
<td>Independence is questionable</td>
<td>Some segregation of duties exists but is inconsistent and one manager oversees both</td>
<td>Staff and reporting lines independent</td>
<td>Clear segregation of duties with different reporting lines through to different senior level executives; clear understanding of necessary controls</td>
</tr>
<tr>
<td>5   External Review and Validation</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5.1  External audit</td>
<td>Not performed, or with known flaws, or performed as a formality</td>
<td>Management and the Board take interest in the audit process and its findings</td>
<td>Management and the Board take interest, seek clarification and act to correct formal and informal findings</td>
<td>Management and the Board seek all benefits of external review and actively use the audit process and its findings to improve governance</td>
</tr>
<tr>
<td>5.2  Other independent/external review and</td>
<td>None</td>
<td>Compliance with key regulatory requirements</td>
<td>Compliance with regulatory requirements, use of independent research and information services, participation in industry associations</td>
<td>All from previous level; use of external rating agencies, external consultants and other independent review providers (e.g. price verification services for illiquid assets)</td>
</tr>
<tr>
<td>validation</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6   Stature of the Risk Management Function</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.1  The CRO's place in the organization</td>
<td>No CRO, or reports to a business line head</td>
<td>Reports to a CFO or non-business line C-level executive</td>
<td>The CRO is a member of the executive board.</td>
<td>The CRO reports directly to the CEO with direct – tested and confirmed - access to the Supervisory Board.</td>
</tr>
<tr>
<td>6.2  CRO pay</td>
<td>CRO is among the lowest paid corporate executives</td>
<td>CRO pay is around the average for the institution's senior management</td>
<td>CRO pay is above the average executive's pay; some incentives for sound risk management</td>
<td>CRO is among the top 5 highest paid executives of the Bank; appropriate incentive structure exists to reward quality of risk management</td>
</tr>
</tbody>
</table>
## Appendix 1: Evaluation Table – Key Risk Governance Principles

<table>
<thead>
<tr>
<th>Benchmarking Criteria</th>
<th>Unsatisfactory</th>
<th>Base Level</th>
<th>Improved Level</th>
<th>Advanced Level</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Evaluation Criteria</strong></td>
<td><strong>6.3 Risk staff remuneration</strong></td>
<td>Risk staff are among the lowest paid; or have incentives to ignore risk in the interest of volume</td>
<td>Risk staff receive average pay within the organization; no incentives for either sound risk management revenue growth</td>
<td>Risk staff receive above average pay with some incentives for sound risk management</td>
</tr>
<tr>
<td><strong>7 Accountability, Disclosure, Transparency</strong></td>
<td><strong>7.1 Board level</strong></td>
<td>No specific accountability measures</td>
<td>Duties explicitly defined but no performance evaluation in place</td>
<td>Duties explicitly defined and performance evaluated periodically</td>
</tr>
<tr>
<td></td>
<td><strong>7.2 Management level</strong></td>
<td>No specific accountability measures</td>
<td>Duties explicitly defined but no performance evaluation in place</td>
<td>Duties explicitly defined and performance evaluated periodically</td>
</tr>
<tr>
<td></td>
<td><strong>7.3 Staff level</strong></td>
<td>No specific accountability measures</td>
<td>Duties explicitly defined but no performance evaluation in place</td>
<td>Duties explicitly defined and performance evaluated periodically</td>
</tr>
<tr>
<td><strong>8 High Ethical Standards</strong></td>
<td><strong>8.1 Policies, Code of Conduct</strong></td>
<td>No reference made to ethical standards in official documents or in any form of corporate communications</td>
<td>Reference made to high ethical standards but no specific discussions or training</td>
<td>Code of conduct exists with some specific guidance on situations and behaviors to avoid; some form of formal agreement to comply is required of all employees</td>
</tr>
<tr>
<td></td>
<td><strong>8.2 Beliefs and attitudes commonly held within the organization</strong></td>
<td>Any act not explicitly prohibited or provable is perceived as acceptable</td>
<td>There are “taboos” that cannot be breached but they are minimal</td>
<td>Fairly well spread awareness of unspoken rules and the need to avoid even the appearance of impropriety</td>
</tr>
</tbody>
</table>
### Standards on Risk Governance in Financial Institutions

#### Benchmarking Criteria

<table>
<thead>
<tr>
<th>Evaluation Criteria</th>
<th>Unsatisfactory</th>
<th>Base Level</th>
<th>Improved Level</th>
<th>Advanced Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.3 Ethically questionable behavior</td>
<td>Numerous incidents reported informally, with no known consequences</td>
<td>Examples exist of punishment or negative consequences for unethical behavior</td>
<td>Questionable behaviors are usually discouraged and punished; some discussion and communication of ethical ambiguities, potential issues and consequences</td>
<td>Questionable behaviors are rare and consistently discouraged and punished; extensive discussion of ethical ambiguities, potential issues, and consequences; appropriate behavior is modeled at the Board and senior management levels and no exceptions are tolerated</td>
</tr>
</tbody>
</table>

#### Pervasive Risk Management Culture

<table>
<thead>
<tr>
<th>9.1 Risk culture in business units</th>
<th>No risk management responsibility perceived, Risk function seen as unnecessary intrusion</th>
<th>Risk management recognized as a business responsibility; need for independent Risk function not understood</th>
<th>Risk management recognized as a business unit responsibility; need for independent Risk function understood; some level of cooperation exists between Business units and Risk function</th>
<th>Business units cooperate routinely with Risk function to achieve optimal balance of risk and return; information flows constructively in both directions</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.2 Risk culture among control units</td>
<td>Duplication, &quot;competition&quot; and isolation among control units</td>
<td>Some coordination exists among control functions but it is informal and inconsistent</td>
<td>There are structures and processes for information exchange but duplication and gaps exist; no practical opportunities for staff to work together</td>
<td>There is a holistic view of risk management with control functions coordinating, routinely sharing information and cooperating to achieve effective risk management of all risks at all levels</td>
</tr>
<tr>
<td>9.3 Risk function’s input to daily business decisions</td>
<td>None</td>
<td>Business lines seek input only to comply with rules</td>
<td>Business lines understand the general risk implications of their decisions and sometimes seek Risk function’s input for clarification and further insight</td>
<td>There is frequent exchange of information and productive debate between business lines and the Risk function, with a clear understanding of each other’s roles and appreciation for their point of view</td>
</tr>
</tbody>
</table>

#### Effective Risk Communication

<table>
<thead>
<tr>
<th>10.1 Regular meetings on risk issues</th>
<th>Do not happen</th>
<th>Happen at high level (Management, Board) up to a few times a year</th>
<th>At least Quarterly at Board level, monthly or weekly at Management level and lower levels</th>
<th>In addition to previous, ad-hoc meetings on specific issues are frequent and productive</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.2 Risk reporting system</td>
<td>Little or none</td>
<td>Some reports with little practical impact – too basic or too bulky and unfocused</td>
<td>Basic package exists covering critical information and used routinely by management in conducting business</td>
<td>Extensive package exists covering a wide spectrum of risk information, adequately prioritized; used routinely as a key management tool</td>
</tr>
</tbody>
</table>
## Appendix 1: Evaluation Table – Key Risk Governance Principles

<table>
<thead>
<tr>
<th>Evaluation Criteria</th>
<th>Benchmarking Criteria</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>10.3</strong> Bank-wide adoption of risk vocabulary and practical use of tools</td>
<td><strong>Unsatisfactory</strong></td>
</tr>
<tr>
<td>None</td>
<td>Some risk concepts, issues, and measures are commonly used</td>
</tr>
<tr>
<td><strong>11</strong> Adequate risk competencies</td>
<td><strong>11.1</strong> Board level</td>
</tr>
<tr>
<td><strong>11.2</strong> Risk management staff</td>
<td>Little relevant education (economics, finance, statistics, banking, IT) or banking products and industry experience</td>
</tr>
<tr>
<td><strong>11.3</strong> Other staff</td>
<td>Little or no risk-related education</td>
</tr>
<tr>
<td><strong>11.4</strong> Ongoing professional development</td>
<td>No programs.</td>
</tr>
<tr>
<td><strong>12</strong> Other Resource Availability</td>
<td><strong>12.1</strong> Risk IT Budget</td>
</tr>
<tr>
<td>None</td>
<td>Basic – mainly Excel/MS Office (or similar)</td>
</tr>
<tr>
<td><strong>12.2</strong> Risk Systems</td>
<td>Unavailable, no effort to collect</td>
</tr>
</tbody>
</table>
Appendix 2: Evaluation Table – Risk Management Organizational Structure

The following table is used for shortcomings identification, tracking progress, and planning activities in strengthening risk governance in the Financial Institutions. Evaluation criteria are applicable to any types of financial institutions and scale of activities. However, benchmarking criteria may vary on risk the financial institution is exposed: the more institution is risk exposed the more level of risk governance it should meet.

<table>
<thead>
<tr>
<th>Evaluation Criteria</th>
<th>Benchmarking Criteria</th>
</tr>
</thead>
<tbody>
<tr>
<td>Board Level</td>
<td></td>
</tr>
<tr>
<td>1.1 Board Risk Committee</td>
<td>Unsatisfactory: No Board member has knowledge of or responsibility for Risk issues.</td>
</tr>
<tr>
<td>2.1 CRO</td>
<td>Unsatisfactory: No senior management oversight of risk.</td>
</tr>
<tr>
<td>3.1 Audit Committee</td>
<td>Unsatisfactory: Does not exist.</td>
</tr>
<tr>
<td>4.1 Credit Committee</td>
<td>Unsatisfactory: No credit committee in place. Credit approvals issued by a single unit or individual within the business line.</td>
</tr>
</tbody>
</table>
## Appendix 2: Evaluation Table – Risk Management Organizational Structure

<table>
<thead>
<tr>
<th>Evaluation Criteria</th>
<th>Benchmarking Criteria</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Unsatisfactory</strong></td>
<td><strong>Base Level</strong></td>
</tr>
<tr>
<td><strong>ALCO</strong></td>
<td></td>
</tr>
<tr>
<td><strong>5.1</strong> ALCO</td>
<td>No ALCO exists.</td>
</tr>
<tr>
<td><strong>Executive Risk Committee</strong></td>
<td></td>
</tr>
<tr>
<td><strong>6.1</strong> Executive Risk Committee</td>
<td>Does not exist.</td>
</tr>
<tr>
<td><strong>Independent Risk Management Function</strong></td>
<td></td>
</tr>
<tr>
<td><strong>7.1</strong> Credit Risk Function</td>
<td>No staff with distinct Credit Risk responsibilities</td>
</tr>
<tr>
<td><strong>7.2</strong> Market Risk Function</td>
<td>No dedicated Market Risk staff</td>
</tr>
<tr>
<td><strong>7.3</strong> Operational/Enterprise Risk Management (OR/ERM) Function</td>
<td>None</td>
</tr>
<tr>
<td>Evaluation Criteria</td>
<td>Unsatisfactory</td>
</tr>
<tr>
<td>---------------------</td>
<td>---------------</td>
</tr>
<tr>
<td>7.4 Methodology,</td>
<td>None</td>
</tr>
<tr>
<td>8 Independent Audit Function</td>
<td></td>
</tr>
<tr>
<td>8.1 Existence and position in the organization</td>
<td>Does not exist</td>
</tr>
</tbody>
</table>
Appendix 3: Evaluation Table – Risk Management Process and Practices

The following table is used for shortcomings identification, tracking progress, and planning activities in strengthening risk governance in the Financial Institutions. Evaluation criteria are applicable to any types of financial institutions and scale of activities. However, benchmarking criteria may vary on risk the financial institution is exposed: the more institution is risk exposed the more level of risk governance it should meet.

<table>
<thead>
<tr>
<th>Evaluation Criteria</th>
<th>Benchmarking Criteria</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1 Risk Identification</strong></td>
<td></td>
</tr>
<tr>
<td>1.1 Access to in-house information (transactions, positions, customers, etc.)</td>
<td>The Risk function has no direct access, relies entirely on departments to self-report. Information comes primarily from IT, Back Office and other control functions, some from business lines, and there is access to key bank systems to obtain some information independently. Information comes largely through independent access to key bank systems, supplemented by information from IT, Back Office and other control functions. Information is freely accessible to the Risk function, through easy-to-use interfaces, with no reliance on other departments and functions for routine information and occasional need for IT or other business-independent departments to supplement.</td>
</tr>
<tr>
<td>1.2 Breadth/depth of information coverage</td>
<td>Minimal details available, many areas not covered. Critical businesses and products are covered, with some level of detail available for drill-down. Critical and most other exposures are identified and reported, with varying levels of depth and detail. All exposures are adequately identified and reported, with multiple levels of detail available for drill-down.</td>
</tr>
<tr>
<td>1.3 Timeliness</td>
<td>Significant delays, no regularity. Mostly available weekly or monthly, some on a regular basis. T+1 (next-day) availability for much of the information. Real time for some of the information, reliable T+1 for the rest, with very few exceptions.</td>
</tr>
<tr>
<td>1.4 Access to market data</td>
<td>None Access to some types of market data is available but there are significant gaps Access is available to most types of market data relevant to the organization but its quality is questionable or its usability is low All necessary market data for relevant markets and products is available to risk management</td>
</tr>
<tr>
<td><strong>2 Risk Assessment</strong></td>
<td></td>
</tr>
<tr>
<td>2.1 Measurement</td>
<td>None Very simple measures such as a low/medium/high scale. Some quantitative measures of risk are used, such as sensitivities to risk factors. Aggregation is basic, not properly accounting for correlations and offsets. A wide range of quantitative risk measures, including probabilistic risk measures and sophisticated aggregation accounting for correlations and offsets between products and business lines.</td>
</tr>
<tr>
<td>Evaluation Criteria</td>
<td>Unsatisfactory</td>
</tr>
<tr>
<td>---------------------</td>
<td>---------------</td>
</tr>
<tr>
<td>2.2 Scenario analysis and stress testing</td>
<td>None</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>3 Risk Reporting</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.1 Report content</td>
</tr>
<tr>
<td>3.2 Reporting frequency</td>
</tr>
<tr>
<td>3.3 Distribution of reports</td>
</tr>
</tbody>
</table>
## Appendix 3: Evaluation Table – Risk Management Process and Practices

<table>
<thead>
<tr>
<th>Evaluation Criteria</th>
<th>Benchmarking Criteria</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>Unsatisfactory</strong></td>
</tr>
<tr>
<td>4</td>
<td>Risk Control/ Mitigation</td>
</tr>
<tr>
<td>4.1 Risk Limits</td>
<td>Few if any risk limits</td>
</tr>
<tr>
<td>4.2 Escalation procedures for excesses and exceptions</td>
<td>Lack of a well-defined procedure for escalation of excesses and exceptions</td>
</tr>
<tr>
<td>4.3 New Product Approval (NPAP)</td>
<td>No such process exists</td>
</tr>
<tr>
<td>4.4 Contingency plans for exceptional situations</td>
<td>No contingency plans</td>
</tr>
</tbody>
</table>
Appendix 4: Terms and Definitions

**Governance** – exercise of political authority and the use of institutional resources to manage society’s problems and affairs. The word *governance* derives from the Greek verb κυβερνάω [kubernáo] which means *to steer.*

**Corporate governance** – the set of decisions and actions that define expectations, regulate relationships, grant power, or verify and evaluate performance within an organization.

**Risk governance** – the subset of corporate governance decisions and actions that ensure effective risk management, including cohesive policies, guidance, processes and decision-rights within the area of risk.

**Risk-based pricing** – using actuarial methods to determine financial prices not only to account for the time value of money, but also to compensate for risk, or potential loss. E.g., an interest rate on a loan would be determined by the lender’s estimate of the probability that the borrower will default on that loan. In the ideal case, when precise estimates are possible, charging the estimated risk-based interest rates for a portfolio of loans would exactly cover (expected) losses from that portfolio. If such precise estimates are impossible to achieve, at a minimum, a borrower who is viewed as less likely to default will be offered a better (lower) interest rate than a higher-risk borrower.

**Risk-adjusted return** – the concept of incorporating a measure of “riskiness” into the measurement of returns, on the broad premise that in economic enterprise, risk is traded off against benefit. See also RAROC and RORAC.

**Risk-based Return on Capital (RAROC)** – a risk-based profitability measurement framework for analyzing risk-adjusted financial performance and providing a consistent view of profitability across businesses. Defined as a ratio: \( \text{RAROC} = \frac{(\text{Expected Return})}{(\text{Economic Capital})} \)

**Return on Risk Adjusted Capital (RORAC)** and **Risk-Adjusted Return on Risk-Adjusted Capital (RARORAC)** – risk-based profitability measurement frameworks used as alternatives to RAROC, whereby the risk adjustment of Capital is based on the capital adequacy guidelines as outlined by the Basel Committee, currently Basel III.

**Economic capital** – the amount of money needed to secure the survival of a financial institution in an extremely adverse scenario (defined at a very low probability level); a buffer against expected shocks in market values. Economic capital is a function of market risk, credit risk, and operational risk, and is often equated to VaR.

**Risk-based capital allocation** – the use of capital based on estimates of risk, generally seen as a method to improve the capital allocation across different functional areas of banks, insurance companies, or any business in which capital is placed at risk for an expected return above the risk-free rate. RAROC as a system allocates capital for 2 basic reasons - risk management and performance evaluation.

**Risk-based performance measurement** – an application of the RAROC framework to assign capital to business units based on the economic value added by each unit.

**Risk-based remuneration (compensation)** – a system of financial incentives for employees and managers of an organization that are designed to encourage prudent risk-taking in the best interest of the organization and to discourage excessive, short-sighted risk-taking.

**Business strategy** – a term that, in the broadest sense, is used to mean Corporate Strategy, i.e., an organization's approach to and plan for doing business which answers the questions “which businesses should we be in?” and “how does being in these businesses add to our competitive advantage and financial success”; in a narrower sense, business strategy relates to individual units within a larger organization.

**Business origination** – the set of functions related to generating business revenues through matching products and clients and concluding transactions, performed by the Front Office.
**Front Office** – a general term referring to a bank’s departments that come into contact with clients and perform revenue generation through business origination - arranging, structuring, pricing and committing new transactions; trading and “first-line” risk assessment; managing client relationships and providing client advisory services. This includes marketing and sales personnel, bankers and client relationship managers, fund managers and research analysts, as well as many technical functions directly supporting business origination (e.g. quantitative analysts who develop financial models for pricing complex transactions).

**Back Office** – includes the Operations, Customer Service, a large part of Information Technology, and possibly other departments and functions. Their roles ensure that transactions are properly processed, documented and accounted for and are within properly approved limits. They carry a mix of support and control functions. They may also monitor internal limits and legal and regulatory compliance at the transaction level, and ensure the maintenance of the IT and support services infrastructure. Reporting lines of staff will be to department heads and then, typically, to a Chief Operating Officer, reporting to the Executive.

**Middle Office** – the definition tends to vary somewhat from bank to bank, but will normally include some control functions and some administration and support for the front office businesses. The term “middle office” has evolved in recent years to focus on departments with key control functions that necessitate close ongoing liaison with front office. These include Product Control and Risk Management which perform important independent profit-and-loss and risk assessments (or control checks on the accuracy of profit-and-loss and risk numbers generated by front office). The criticality of an independent assessment and control of the activities of the front office makes it imperative to establish independent reporting lines for the Middle Office function.

**Dedicated Risk (Management) function** – a department within a financial institution that performs independent assessment of the risks undertaken by Front Office on behalf of the organization through business origination, as well as of other risks arising in the course of doing business.

**Independent Risk (Management) function** – see Dedicated Risk (Management) function.
Appendix 5: References

1. Principles for enhancing corporate governance, BIS, Working Group on Corporate Governance of the Basel Committee on Banking Supervision, October 2010

2. Corporate governance in financial institutions and remuneration policies, Green Paper, European Commission, Brussels

3. Corporate governance in financial institutions: the lessons to be learnt from the current financial crisis and possible steps forward, European Commission Staff Working Paper


5. Basel Committee on Banking Supervision, Enhancing corporate governance for banking organisations, September 1999. Revised in February 2006

6. OECD, Guidelines for insurers’ governance, 2005

7. OECD, Revised guidelines for pension fund governance, July 2002


10. CEBS High Level Principles for Risk Management, EBA (European Banking Authority)’s Committee of European Bank Supervisors, 16 February 2010

11. OECD’s public consultation ‘Corporate governance and the financial crisis’, 18 March 2009

12. G20 declaration of 15 November 2008

13. Principles for Sound Compensation Practices (FSB Principles) and accompanying Implementation Standards (FSB Standards), Financial Stability Board

14. Committee of Sponsoring Organizations (COSO) Enterprise Risk Management (ERM) framework


17. US Sarbanes Oxley Act


20. MiFID Markets in Financial Services Directive


22. OECD’s Principles of Corporate Governance, 2004

23. PRMIA Risk Governance Principles


25. Risk Management, Corporate Governance, and Bank Performance in the Financial Crisis, paper by Vincent Aebia, Gabriele Sabatob, and Markus Schmid, January 2011
International Finance Corporation
Financial Market Crisis Response Program in
Eastern Europe and Central Asia

1, Dniprovsky Uzviz, 3rd floor Kyiv, 01010, Ukraine
Phone: +38 044 490 6400
Fax: +38 044 490 6420
www.ifc.org/eca/cr