Risk Culture, Risk Governance, and Balanced Incentives

Recommendations for Strengthening Risk Management in Emerging Market Banks

IN PARTNERSHIP WITH

First printing, August 2015

IFC, a member of the World Bank Group, creates opportunity for people to escape poverty and improve their lives. We foster sustainable economic growth in developing countries by supporting private sector development, mobilizing private capital, and providing advisory and risk mitigation services to businesses and governments.

Acknowledgements

This report was commissioned by IFC through its Global Risk Management Advisory Program within the Financial Institutions Group. The program's objective is to strengthen financial institutions' risk management capacity and frameworks, while helping to support MSMEs access sustainable and responsible financial services in emerging markets by taking a comprehensive approach that focuses on all aspects of sound risk management including risk governance, market risk, liquidity risk, credit risk, operational risk, asset liability management, and capital adequacy. The program aims to demonstrate that growth and resilience to financial crises requires implementation of better risk management systems and processes.

The report "Risk Culture, Risk Governance, and Balanced Incentives: Recommendations for Strengthening Risk Management in Emerging Market Banks" was developed under the overall guidance of Cameron Evans and Shundil Selim. The team would like to acknowledge the contribution of IFC's internal peer reviewers: Garth Bedford, Charles Travis Canfield, and Kiril Nejkov.

IFC would like to particularly thank the team at Deloitte, who were commissioned by IFC to produce this report. The Deloitte team was led by Julie Nyang'aya and included Urvi Patel and Crispin Njeru. Deloitte is the brand under which tens of thousands of dedicated professionals in independent firms throughout the world collaborate to provide audit, consulting, financial advisory, risk management, tax and related services to select clients. These firms are members of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL").

IFC would especially like to acknowledge and thank the Government of Japan for their contribution and partnership in the Global Risk Management Advisory program and this report.

Table of Contents

Abbreviations ii

1 Executive Summary 1

2 Risk Culture in Banks 7

2.1 Introduction 7

2.2 Best Practices in Risk Culture 10

2.3 Risk Culture Maturity Rating Scale 20

2.4 Conclusion 21

3 Risk Governance in Banks 22

3.1 Introduction 22

3.2 Best Practices in Risk Governance 24

3.3 Risk Governance Maturity Rating Scale 42

3.4 Conclusion 44

4 Incentive Programs in Banks. 45

4.1 Introduction 45

4.2 Best Practices in Balanced Incentive Programs at Banks. 46

4.3 Balanced Incentives Program Maturity Rating Scale 53

4.4 Conclusion 55

5 Conclusion. 56

6 Appendix 1: Implementing the Best Practices 58

7 Working Definitions 63

8 Annexes 65

Annex 1: Illustrative Code of Conduct 65

Annex 2: Illustrative Whistle-Blower Policy 70

Annex 3: Illustrative Board Risk Committee Charter 72

Annex 4: Illustrative Terms of Reference for a Chief Risk Officer 75

Annex 5: Illustrative Risk Appetite Statement 76

Annex 6: Illustrative Training Program for the Board of Directors 77

Annex 7: Illustrative Training Program for Risk Champions 78

Annex 8: Illustrative Board Risk Committee Evaluation Questionnaire 79

9 References 81

Abbreviations

BAC	Board Audit Committee
BARC	Board Audit Review Committee
BIRMC	Board Integrated Risk Management Committee
BRMC	Board Risk Management Committee
CAE	Chief Audit Executive
CBRC	China Banking Regulatory Commission
CCO	Chief Compliance Officer
CEO	Chief Executive Officer
CFO	Chief Finance Officer
CRO	Chief Risk Officer
EBITDA	Earnings Before Interest, Tax, Depreciation and Amortization
ERM	Enterprise Risk Management
ESMA	European Securities and Markets Authority
ESOP	Employee Share Ownership Plan
EU	European Union
FCA	Financial Conduct Authority
FSA	Financial Services Authority
FSB	Financial Stability Board
FSI	Financial Services Industry
GFSI	Global Financial Services Industry
ICAAP	Internal Capital Adequacy Assessment Process
ICT	Information and Communication Technology
IFC	International Finance Corporation
IIA	Institute of Internal Auditors
IIF	Institute of International Finance
IMF	International Monetary Fund
IRGC	International Risk Governance Council
IRM	Institute of Risk Management
ISO	International Standards Organization
IT	Information Technology
KPI	Key Performance Indicator
KRI	Key Risk Indicator
LIBOR	London Interbank Offered Rate
MSME	Micro, Small, and Medium Enterprises
PRA	Prudential Regulation Authority
RAF	Risk Appetite Framework
RAS	Risk Appetite Statement
RCSA	Risk and Control Self-Assessment
SME	Small and Medium Enterprises
USD	United States Dollar

1 Executive Summary

1.1 BACKGROUND

The International Finance Corporation (IFC), as a member of the World Bank, believes that sound, inclusive, and sustainable financial markets are essential to building shared prosperity and ending extreme poverty. Access to finance is a key barrier to the growth of Small and Medium Enterprises (SMEs) and the establishment of micro-enterprises. The access to finance gap in emerging markets is large—2 billion adults do not have access to savings or credit, while 200 million micro, small, and medium enterprises (MSMEs) do not have access to credit. Working through financial intermediaries enables IFC to encourage them to become more involved in sectors which are strategic priorities such as women-owned businesses, climate change, and agriculture and in underserved regions such as fragile and conflict-affected states as well as in housing, manufacturing, infrastructure, and social services. Our work with these clients has supported an estimated 100 million jobs. Through its Advisory Services, IFC has also scaled up the sustainable provision of financial services in developing countries by addressing systemic issues such as credit information and credit bureaus, improvements in risk management, corporate governance, and the introduction of environmental and social standards.

The global financial turmoil which set in half a decade ago, and whose impact continues to be felt through a sluggish global economy, has affirmed the importance of sound financial systems, and in particular the role which effective risk management plays in ensuring sustainable growth of an economy. The Euro and United States of America (US) subprime crises have demonstrated that even within a tightly regulated financial system, hard-earned growth can be easily eroded in the absence of certain aspects of good governance principles and management practices. A key area of attention that has emerged from the diagnosis of the financial crisis is the critical importance of risk culture, risk governance, and balanced incentives within financial institutions as preconditions for maintaining an effective risk management framework. A lot of research and studies have been done on the impact of these three components with a focus on the failures in developed markets and on large banks. There has been little or no focus on the impact of similar issues in emerging markets.

The IFC Global Risk Management advisory program aims to strengthen financial institutions' risk management capacity and frameworks and has published this best practice handbook to expand the knowledge and research on practices on risk culture, risk governance, balanced incentives, and the impact these three components have on effective

The global financial turmoil which set in half a decade ago, and whose impact continues to be felt through a sluggish global economy, has affirmed the importance of sound financial systems, and in particular the role which effective risk management plays in ensuring sustainable growth of an economy. The Euro and United States of America (US) subprime crises have demonstrated that even within a tightly regulated financial system, hard-earned growth can be easily eroded in the absence of certain aspects of good governance principles and management practices.

risk management. A number of studies[1] have already been published on the impact of these three components, with a focus on the failures, practices, and trends in developed markets and on large banks, particularly in North America and Europe. This handbook, therefore, focuses on providing guidelines and references to assist banks in emerging markets and includes examples of current practices in these regions

1.2 ABOUT THE HANDBOOK

This handbook was developed through research and consolidation of guiding principles as published by various authoritative sources. These sources include the Basel Committee on Banking Supervision, International Monetary Fund (IMF), European Securities and Markets Authority (ESMA), Financial Services Authority (FSA) UK, which has since April 2013 been redesigned to create the Prudential Regulation Authority (PRA) and Financial Conduct Authority (FCA), the World Bank, the Institute of International Finance (IIF), the European Banking Authority (EBA), Financial Stability Board (FSB), professional services organizations publications, as well as bank regulators in various regions.

The above research has been complemented through the inclusion of case studies. Case study examples included in this handbook were obtained from discussions and questionnaires completed by local banks operating in emerging markets and from publicly available information. Indigenous banks from the six emerging market regions of East Asia and Pacific, East Europe and Central Asia, Latin America and the Caribbean, Middle East and North Africa, South Asia, and Sub-Saharan Africa were invited to participate in the research that guided the development of this handbook. The banks' responses were voluntary. The handbook therefore includes case studies on particular risk management practices from representative banks in the regions that opted to participate. The participating institutions ranged from commercial banks offering retail and corporate banking services to SMEs (including microfinance institutions) to listed and large state-owned banks with extensive regional networks.

1 Accenture, *Global Risk Management Study*, 2013, indicated having 61% responses from North America and Europe, KPMG's *Expectations of Risk Management Outpacing Capabilities: It's Time for Action,* 2013, had 50%, Ernst & Young, *Remaking Financial Services: Risk management five years after the crisis: A survey of major financial institutions*, 2013, had 56%, and Deloitte & Touche LLP, *Global risk management survey, eighth edition: Setting a higher bar,* 2013, had 58% respondents from developed markets.

The approaches provided in this handbook are complementary to a bank's existing risk management practices and framework and can provide a useful tool and guide for banks to further improve the effectiveness of their risk management activities. In risk management, there cannot be a "one size fits all" solution, and therefore recommendations provided should be tailored to fit each bank's size, complexity of business, and any other rules, regulations, and guidelines provided by the bank's regulator.

1.3 BENEFITS OF THE HANDBOOK

The handbook provides some answers to the following questions that have been in the forefront of the Financial Services Industry (FSI) and especially banks in their pursuit of effective risk management programs:

- What are the key characteristics of the "softer" qualitative factors of risk culture, risk governance and balanced incentives? What is their impact on effective risk management?
- Is there a way for a bank or a third party to benchmark or to assess these factors? Upon assessment, how can these factors be implemented?

The handbook has incorporated assessment tools and maturity rating scales which banks or third parties such as investors can use to benchmark a bank's risk policies against best practices and to identify gaps within its existing risk management practices in the areas of risk culture, risk governance, and balanced incentives.

Lastly, the handbook contains an implementation guide included under Chapter 6, Appendix 1, which provides systematic guidance on how banks can achieve their desired risk culture, risk governance, and balanced incentives plans so as to support their risk management programs. The guide encompasses an approach on current assessment of a bank's practices, implementation of desired practices, and continuous monitoring and improvement of the bank's practices.

1.4 SECTIONS OF THE HANDBOOK

The handbook is divided into three chapters, which focus on best practices in risk culture, governance, and incentives and their impact on effective risk management. Each chapter discusses the best practices in each of these areas along with a maturity rating scale that can help organizations undertake

a self-assessment against defined qualitative maturity assessment factors.

Risk culture is a good indicator of how widely a bank's risk management policies and practices have been adopted.[2] It encompasses the general awareness, attitudes, and behaviors of the bank's Board of Directors, senior management, and employees toward risk. In its journey toward effective risk management, a bank should first understand its existing risk culture and measure how well it supports the organization's risk strategy and risk management approach. Various tools, such as the Risk Culture Framework, can help banks understand their existing risk culture.[3] The Risk Culture Framework (see Figure 1) provides details of risk culture drivers and subcomponents. The framework consists of four drivers: risk competency, organization, relationships, and motivation.

To enhance the understanding of risk culture and its inter-relationship with risk governance and balanced incentives, banks should consider the following key culture influencers:[4]

- **Risk Competence:** This encompasses the bank's recruitment, learning, skills, and knowledge in relation to risk. A bank can build on its existing risk competence through:
  - **a. Skills:** The Board of Directors, senior management, and employees should have skills for risk identification, assessment, and identifying mitigating actions. Regular training can enhance risk management skills of these individuals across the bank, particularly with regard to best practices, regulatory requirements and knowledge of the bank's key policies, processes and standards.
  - **b. Learning:** The bank should propagate knowledge of risk management to all its employees, senior management, and Board of Directors. To cope with the changing risk dynamics, a bank should have formal learning programs where the Board of Directors, senior management, and employees are required to learn risk management practices. The Human Resources or related department should work with the risk management function to identify or design suitable programs that enhance the Board of Directors, senior management, and bank employees' risk management capabilities within the context of the bank. The learning programs should be continually reviewed for relevance.
  - **c. Recruitment and Induction:** The bank's recruiting process should take into consideration a prospective Board member or employee's predisposition toward risk, plus their current knowledge and past experience on risk management. The bank's induction programs for Board members and employees should include training on risk management to ensure that new employees and Board members are properly oriented on the bank's view toward risks.
- **Organization:** These are the processes, procedures, and governance systems that support risk management. It is how the bank's operating environment is structured and what is valued.
  - **a. Strategy and Objectives:** The bank should have clearly stated objectives. As part of the process of determining these objectives, the bank should identify the risks it faces and define an acceptable risk profile in its risk appetite statement. This is an iterative process whereby there is continuous assessment and evaluation of the risks and their potential implications within the strategy, objective, planning and oversight activities.

Figure 1: Risk culture framework

Adapted from Deloitte, *Cultivating a Risk Retirement Culture* (2012).

2 Deloitte, *Cultivating a Risk Intelligent Culture: Understand, measure, strengthen, and report*, 2012, p. 3.

3 Ibid., p. 2.

4 Ibid.

b. **Values and Ethics:** It is important that all bank personnel (i.e., Board members, management and employees) do not expose the bank to imprudent risk taking by working outside of the bank's defined ethical principles. The bank should outline its value systems and encourage commitment by all to ensure the application of defined ethical principles in all business activities when making decisions. This may be extended to the activities of partnerships and relationships beyond bank personnel, such as, for example, outsourced service providers.

c. **Policies, Processes and Procedures:** The bank's policies, processes and procedures should have sufficient management controls to promote prudent risk taking by employees within the acceptable risk appetite parameters. The policies, processes, and procedures should support holistic risk management and highlight the roles and responsibilities of each employee in the risk management process.

- **Relationships:** These are the interactions between the different hierarchical levels within the bank in areas specifically covering ethics, management, leadership behavior and communication flows. Banks can strengthen relationships through enhanced communication and constructive challenge in the following areas:

  a. **Effective Communication:** Good corporate governance requires that risks are understood, managed and, where appropriate, communicated.[5] There should be structured communication channels to ensure effective risk reporting within the bank and, where necessary, with external parties. The bank's employees should be encouraged to identify and report on existing and emerging risks through a clearly defined escalation process. Communication also helps inform the whole bank of the importance placed by top management on staff having the right risk culture.

  b. **Leadership:** The Board of Directors and senior management should be the main drivers of embracing the right risk culture. Whereas the Board of Directors sets the tone for risk management practices, senior management should support sound infrastructure and processes for risk management and should provide the appropriate tools to employees for successful risk management. It is important that business unit managers understand their responsibilities and, through the examples they set, promote and influence lower level employees to embrace the right risk culture.

  c. **Challenge:** The bank should encourage constructive challenge on risk-related discussions. There should be an enabling environment for such two-way discussions across all functions and between the various levels in the bank from the Board to executives, managers to employees, peer to peer, and the risk function to the business. This challenge should be seen as a valuable and constructive activity without fear of reprisal.

- **Motivation:** This is the analysis of why people manage risks the way they do, how risk is taken into account in performance management, risk appetite, incentives, and obligations. Banks should align motivation systems through:

  a. **Performance Management:** The bank should align its performance management systems toward prudent risk taking by senior management and employees. The Key Performance Indicators (KPIs) of senior management should include risk management measures, which should have an appropriate weighting to ensure they influence the right behavior.

  b. **Risk Orientation:** There should be a common risk language throughout the bank. The Board and senior management should ensure that all employees understand and live the bank's risk appetite statement. The nature of risks an employee is likely to take helps gauge his or her risk orientation. The bank should also ensure that its incentive mechanisms promote prudent risk taking among its senior management and employees.

  c. **Accountability:** The risk function in a bank should constantly inform business units of the importance of risk management. Business units and employees within those functions should be held liable for any imprudent risks taken by them. Employee risk taking should be premised on the bank's risk appetite and be in line with the approach to risks managed by the bank. The Board as whole, senior management, and each employee should be held accountable, individually and/or collectively, for imprudent risks taken.

The subcomponents of this model have been used to develop the best practices in risk culture, risk governance, and balanced incentives as included in this handbook.

5 OECD, *Risk Management and Corporate Governance,* 2014, p. 7.

Table 1: Relationships between risk culture, risk governance, and balanced incentives

	Elements	Risk Culture	Risk Governance	Incentive Program
Risk Competence	Skills	x	x	
	Learning	x	x	
	Recruitment and Induction	x	x	
Organization	Strategy and objectives		x	
	Values and ethics	x		
	Policies, procedures and processes		x	x
Relationships	Challenge	x	x	
	Leadership	x	x	
	Communication	x	x	x
Motivation	Performance management	x	x	x
	Risk orientation	x	x	x
	Accountability	x	x	x

Table 1 shows the interrelationships between the risk culture framework elements as described above and the aspects of risk culture, risk governance, and balanced incentives.

1.4.1 CHAPTER TWO: RISK CULTURE IN BANKS

An effective risk culture implies that the Board, senior management, and employees understand the bank's approach to risks and take personal responsibility to manage risks in everything they do and encourage others to follow their example. A bank should encourage the Board, senior management, and employees to make the right risk-related decisions and exhibit appropriate risk management behavior by aligning its management systems and behavioral norms.

Creating an effective risk culture requires Boards and senior management to focus on the bank's written rules that clearly define risk management objectives and priorities and by taking a hard, honest look at any informal rules, protocols, the way workflows are performed, how decisions are made, and the link to the bank's compensation practices. Often, it is these informal rules, practices and procedures that are strong influences in guiding people's behavior. In doing this, Board members and senior management are responsible for setting the right tone at the top and for cultivating a bank-wide awareness of risks that fosters risk intelligent behavior at all levels of the bank.

Risk intelligence is the ability of a bank and its employees to distinguish between two types of risks: the risks that should be managed to prevent loss or harm; and the risks that must be taken to gain competitive advantage. It provides a bank with the ability to translate risk insights into superior judgment and practical action to improve resilience to adversity as well as improve agility to seize opportunities.

A bank's risk culture is not a stand-alone component in its efforts toward effective risk management, but is intertwined with its risk governance practices as well as its incentive programs. Chapters two and three of the handbook further discuss risk governance practices and balanced incentive programs, respectively.

1.4.2 CHAPTER THREE: RISK GOVERNANCE IN BANKS

Risk governance refers to the principles of good governance applied to the identification, management and communication of risk. It incorporates the principles of accountability, participation and transparency in establishing policies and structures to make and implement risk-related decisions.[6]

6 International Finance Corporation, *International Finance Corporation Control Environment Toolkit: Risk Governance, Model Risk Management Committee Charter*, 2013, Sec. 2.1.25 (internal document on file with IFC).

For a bank to reap the benefits of effective risk management, the Board and senior management must show commitment to their risk governance responsibilities, which in turn influence the risk culture of the bank. While every employee in the bank plays a role in risk management, the oversight role of risk management and establishing the framework for good governance lies squarely with the Board.

A sound risk governance framework promotes clarity and understanding of the bank's risk appetite and the ways in which bank employees execute their responsibilities. Risk governance should cover all aspects of risk management, which includes setting the bank's risk appetite, risk identification, risk assessment or measurement, prioritization, mitigation actions, and continuous monitoring. The Board and senior management should define and assign responsibility for these risk management functions to ensure that all the functions are carried out effectively and efficiently. Effective risk governance is key to embedding the right risk culture in a bank as it clarifies the roles and responsibilities of its employees.

Incentives also play an important role, as they help shape employees' attitudes toward assuming risk. Due to this interrelationship, risk culture, risk governance and balanced incentives have an interdependent relationship in their role of ensuring effective risk management programs. Chapter three of the handbook discusses incentive programs.

1.4.3 CHAPTER FOUR: INCENTIVE PROGRAMS IN BANKS

Building value for a bank requires effective risk taking, whether it is taking prudent risks to gain a competitive advantage or mitigating risks to avoid potential losses. The global financial crisis brought to the forefront the important role incentives play in shaping senior management and employees' actions. A bank should aim to match incentives paid (or promised) to senior executives and employees with the risk being taken and the effective management of it to promote the achievement of its long-term objectives. Banks around the globe, and especially those in emerging markets and whose products, operations and complexity are steadily increasing, should learn from the global financial crisis and incorporate risk performance into their incentive programs.

Effective incentive programs within a bank aim to strike a balance between the bank's practices, banking laws and regulations, fluctuating market conditions, and public perceptions. The Board has the responsibility of ensuring that the bank's incentive compensation programs will support the pursuit of the bank's long-term objectives. The Board should have an active role in the determination of the incentive compensation programs, and the potential impact on behavior, for the Board members, senior management, and all other employees.

2 Risk Culture in Banks

Risk culture is based on particular beliefs and assumptions. These can be clustered according to specific cultural tenets, including risk, integrity, governance and leadership, decision-making, empowerment, teamwork, responsibility and adaptability. These tools are expressed in everyday workplace practices through attitudes and behaviors, and when they are expressed by leaders, they serve as powerful (human) culture embedding mechanisms.

At a Glance

Recommended best practices in Risk Culture

- Common Values
- Tone at the top
- Common risk language
- Application of risk management principles
- Timely, transparent and honest risk communications
- Risk management responsibilities
- Challenging discussions on risk management
- Risk reporting and whistle-blowing

2.1 INTRODUCTION

There cannot be a "one size fits all" solution to risk management—however, the method an organization uses to manage risks should align with and support its strategy, business model, business practices and risk appetite and tolerance. This is especially true for banks, where significant risk-based decisions are made throughout the organization on a daily basis. This has given the concept of enterprise risk management (ERM) to become more relevant, especially after the global financial crises.

ERM is a process, effected by the bank's Board of Directors, senior management, and employees, applied in strategy setting and across the bank, designed to identify potential events that may affect the bank and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of its objectives.

The argument on the importance of culture to a bank's enterprise-wide risk management processes and compliance standards would be supported by many. It ensures the following:[7]

- The Board and senior management consider the bank's risk appetite in evaluating strategic alternatives, setting related objectives, and developing mechanisms to manage related risks;
- Enhanced risk response decisions by providing the process to identify and select among alternative risk responses—risk avoidance, reduction, sharing, and acceptance;
- Reduced operational losses or surprises by enhancing the capability to identify potential events and establish responses, reducing surprises and the associated costs or losses;
- By identifying and managing multiple and cross-functional risks, the bank has effective responses to the interrelated impacts, and integrated responses to multiple risks;

7 Adapted from Committee of Sponsoring Organizations of the Treadway Commission, *Executive Summary: Enterprise Risk Management—Integrated Framework*, 2004, pp. 1–4.

Case Study 1: An example of negative culture impact[a]

The London Interbank Offered Rate (LIBOR) is an interest rate at which banks lend unsecured funds to each other and is published daily by the British Bankers' Association (BBA). Each morning, global banks submit their borrowing costs to the Thomson Reuters data collection service and after removing the highest and lowest 25 percent of the submissions, the calculation agent averages the remaining submissions to determine LIBOR. LIBOR is considered the most important benchmark interest rate as many banks use LIBOR to set the interest rates for lending to consumers and businesses. When LIBOR rises, the rates and payments on loans often increase.

Some European banks were recently under investigation for allegedly manipulating the LIBOR rate. The employees of the banks submitted rates that would benefit the banks instead of the rates the banks actually paid for the funds they borrowed. One particular European bank manipulated LIBOR downward to appear less risky. In another European bank, its senior management took the blame for creating a system in which its employees were awarded huge bonuses if they took part in the scheme. Their focus on short-term return on equity and their competitive position led to a decline in culture and values.

This practice undermined investors' confidence in the financial markets and distorted the pricing of trillions of dollars of financial instruments. The banks that participated in the LIBOR scandal have been sued with some paying huge amounts in settlement claims. There has also been a push to scrap the LIBOR rate in favor of a new rate based on real transactions data.

a Alessi, C., Sergie, M.A., *Understanding the Libor Scandal* <http://www.cfr.org/united-kingdom/understanding-libor-scandal/p28729> 5 December 2013 [viewed on 11 November 2014].

- By considering a full range of potential events, senior management is positioned to identify and proactively realize opportunities; and
- Obtaining robust risk information allows senior management to effectively assess overall capital needs and enhance capital allocation.

Identifying what factors make a bank's risk culture strong and how these factors can be aligned with risk and compliance initiatives can, however, be a challenge. Even more challenging is how banks can go about improving their risk culture and measuring progress over time.

To a large degree, a bank's culture may influence how it manages risk when under stress. The risk culture of some banks as shown above can be a negative force, while for other banks it can provide both stability and a competitive advantage.

2.1.1 RISK CULTURE

Culture is amorphous; it is both visible and invisible. Culture shapes the way people act on a daily basis, and influential people inside and outside of an organization can shape it, too. It is often visible through the choices and actions people make. At other times, it is not evident, as some of the cultural drivers and ethos operate "below the surface." Nevertheless, they too influence choices and actions.[8] It is usually a mix between the formal and informal practices and processes that shape banks' decisions.

The bank's Board of Directors and senior management must demonstrate behavior consistent with the desired risk culture. They set the tone at the top, which trickles down to the employees and shapes their behavior. In cases where top management does not show commitment in driving the risk agenda, risk management may remain mere talk with inadequate people, systems and resources in the risk management functions, thus leading to an ineffective risk management program.

The Board of Directors and senior management should ensure early identification and escalation of business risks and promote activities toward ensuring that the employees understand the bank's risk culture. This is possible through clearly defining and assigning roles and responsibilities on risk management functions.

8 Deloitte, *Culture in banking: Under the microscope*, 2013, p. 4.

Illustrative responsibilities in risk management include:[9]

Responsibilities of the Chief Executive Officer (CEO)/Board:

- Determine strategic approach to risk and set risk appetite;
- Establish the structure for risk management;
- Understand the most significant risks; and
- Manage the bank in a crisis.

Responsibilities of the Chief Risk Officer (CRO):

- Develop the risk management policy and keep it up to date;
- Document the internal risk policies and structures;
- Coordinate the risk management (and internal control) activities; and
- Compile risk information and prepare reports for the Board.

Responsibilities of the risk management function:

- Assist the company in establishing specialist risk policies;
- Develop specialist contingency and recovery plans;
- Keep up to date with developments in the specialist area; and
- Support investigations of incidents and near misses.

Responsibilities of the Chief Audit Executive (CAE):

- Develop a risk-based internal audit program;
- Audit the risk processes across the organization;
- Receive and provide assurance on the management of risk; and
- Report on the efficiency and effectiveness of internal controls.

Responsibilities of the business unit manager:

- Build risk aware culture within the unit;
- Agree risk management performance targets;
- Ensure implementation of risk improvement recommendations; and
- Identify and report changed circumstances/risks.

Responsibilities of individual employees:

- Understand, accept and implement risk management (RM) processes;
- Report inefficient, unnecessary or unworkable controls;
- Report loss events and near-miss incidents; and
- Cooperate with management on incident investigations.

Facts or supporting analyses, including a holistic risk impact assessment, should form the basis of decision making in a bank. The bank should see the risk function as a strategic business partner to the business units, facilitating sharing of knowledge and good practices.

2.1.2 RISK INTELLIGENT CULTURE

To embed an effective risk culture in the bank's practices, the bank should aspire to reach a risk intelligent culture status. This implies that everyone in the organization understands the bank's approach to risks, takes personal responsibility to manage risks in everything they do and encourage others to follow their example. A bank's management systems and behavioral norms should encourage people to make the right risk related decisions and exhibit appropriate risk aware behavior.

In doing this, boards of directors and senior management are responsible not just for setting the right "tone at the top," but also for cultivating an enterprise-wide awareness of risks at all levels of the bank.

Experience shows that culture change invariably follows behavior change, especially in critical positions. To jump-start the journey to risk awareness, it is far more effective to pull levers that affect how employees act—such as rewards, roles and responsibilities, and training—than to rely on pronouncements and processes alone to drive the desired change in behavior.

Critical drivers of effective risk culture should be monitored and managed just as conscientiously as any other driver of enterprise value. Formal assessments through surveys and interviews can help Boards and senior management understand their bank's existing cultural norms and ways to influence them. The more a leader can become part of the bank's culture rather than holding himself or herself above it, the better he or she will be able to understand its strengths, identify potential weaknesses, and develop strategies to keep the bank on the right track. It is also critical to align the bank's unwritten rules with its formal, written ones through constant reinforcement of the "right" way to behave. During a recent study—Culture in Banking—bankers rated the leaders of the business units as bearing most

9 Adapted from The Association of Insurance and Risk Managers, *A structured approach to Enterprise Risk Management (ERM)*, 2010, p. 12.

responsibility for setting and changing the culture, followed by the Chief Executive Officer (CEO), the Board of Directors (the Board) and the CRO, in that order.[10] This reflects a known finding in social psychology; that humans tend to conform to the behavior they see around them. Even with the Board taking overall responsibility for risk management, culture behaviors exhibit themselves in day-to-day operations—hence the higher perceived responsibility for those undertaking day-to-day management activities in the bank. When the Board does not set the correct tone for managing risks, risk awareness within the bank may be limited, as there is little or no sharing of information, concerns, and risk impacts within the bank.

Culture, while not easy to master, is crucially important in taking risk management beyond the mechanical articulation of rules and regulations. In the end, culture is what makes risk aware behavior "the way we really do things around here." The bank should recognize that the pursuit of its objectives inevitably means exposure to risk, and therefore the Board should take responsibility for addressing risk with every decision they make. The best practices provided in this handbook would ensure the following nine principles of a risk intelligent organization are applied in a bank with the right risk culture:[11]

- A common definition of risk, which addresses both value preservation and value creation, is used consistently throughout the bank;
- A common risk framework supported by appropriate standards is used throughout the bank to manage risks;
- Key roles, responsibilities, and authority relating to risk management are clearly defined and delineated within the bank;
- A common risk management infrastructure is used to support the business units and functions in the performance of their risk responsibilities;
- Governing bodies (e.g., Board, Board Audit Committee, Board Risk Committee, etc.) have appropriate transparency and visibility in the bank's risk management practices to discharge their responsibilities;
- Senior management is charged with primary responsibility for designing, implementing, and maintaining an effective risk program;
- Business units are responsible for the performance of their business and the management of risks they take within the risk framework established by the senior management;
- Certain functions (e.g., HR, finance, IT, tax, legal, etc.) have a pervasive impact on the business and provide support to the business units as it relates to the bank's risk program; and
- Certain functions (e.g., internal audit, risk management, compliance, etc.) provide objective assurance as well as monitor and report on the effectiveness of a bank's risk program to governing bodies and senior management.

2.2 BEST PRACTICES IN RISK CULTURE

Financial Services Industry (FSI) stakeholders such as governments, regulators, industry bodies, shareholders, and bankers have done much soul-searching since the global financial crisis of 2007/2008 to understand what went wrong and how they can prevent the crisis from happening again. The scale of the crisis led to the questioning of the strength of financial institutions and the suitability of regulatory and supervisory systems that deal with the ever-evolving financial products in the global world. Of particular importance were the following factors that indicated the absence of the "right" risk culture:[12]

- Lack of understanding of the risks and insufficient training for employees;
- Lack of authority of the risk management function;
- Lack of expertise or experience of the employees in the risk management function; and
- Lack of real-time information on risks.

Creating the "right" culture has the potential to do more than merely fix problems. The right culture can provide banks with a competitive advantage that is difficult for rivals to emulate. Getting the culture right may not be the ultimate panacea to all the bank's challenges. However, an effective risk culture can serve as glue that binds together elements such as governance, risk management, compliance, high-level systems and controls, and makes the bank cohesive and stronger.

The following recommended best practices when adopted by a bank, can act as enablers to a risk culture, which would improve the overall effectiveness of its risk management programs:

10 Deloitte, *Culture in banking: Under the microscope*, 2013, p. 21.

11 Deloitte, *Cultivating a Risk Intelligent Culture: Understand, measure, strengthen, and report*, 2012, p. 7.

12 European Commission, *Corporate governance in financial institutions and remuneration policies*, 2010, p. 7.

- **A common purpose, values and ethics:** The Board of Directors, senior management, and employees should clearly understand the purpose for the bank's existence, values, and ethics.
- **The right tone at the top:** The Board of Directors and senior management should take responsibility for risk management, and their actions should indicate their support of the same.
- **Common understanding of risk management terms:** There should be a consistent way of defining and understanding risks across the bank.
- **Universal application of risk management principles:** The Board of Directors, senior management, and employees should apply risk management principles consistently as they make their day-to-day decisions.
- **Timely, transparent, and honest communications on risks:** The bank should ensure that both internal and external stakeholders are informed of the key risks facing the bank and the mitigating controls or strategies in place to address the risks identified.
- **Risk management responsibility:** Risk management is everyone's business and should be seen this way across the bank.
- **Expectations of challenging discussions around risk management:** Conversations around risks facing the bank should be encouraged, as well as an environment that supports open, iterative discussion and debate of the risks.
- **Risk reporting and whistle-blowing mechanism:** The bank should have processes for risk reporting to the Board and other relevant key stakeholders. Mechanisms for whistle-blowing should be encouraged within the bank.

2.2.1 COMMONALITY OF PURPOSE, VALUES, AND ETHICS IN THE BANK

Checkpoint:

- ✓ The bank has a code of conduct
- ✓ Sign off on the code of conduct

A bank's Board of Directors, senior management, and employees have a duty and responsibility to be accountable to their employers, customers, depositors, creditors, colleagues, the banking profession itself, regulators, and the public.

To facilitate commonality of purpose, values, and ethics as a means of enhancing the bank's risk culture, the bank should define and establish a code of conduct to act as a guide for application in specific situations.

The code of conduct (See Annex 1 for an illustrative Code of Conduct) creates a common culture as the bank's employees know and understand the bank's expectations of them. It provides guidelines that employees follow when faced with difficult business decisions and improves the reputation of the bank, as its stakeholders are aware of its corporate values. The code provides protection to the bank if a Board member, senior manager, or employee commits a criminal act in the bank's name. The following are guidelines a bank should undertake to develop an effective code of conduct:

- The code should be simple, principles-based, concise, and written in language that is easily understood by all the bank's employees;
- The code should not include any legal language;
- The code should apply to all Board members, senior management, and employees, regardless of one's hierarchy within the bank;
- The code should be developed by a cross-functional team so as to address all relevant areas, have buy-in across the bank, and represent the bank's institutional values. The team should include representatives from human resources, risk management, internal audit, communications, legal, and any other function that may be deemed important; and
- The code should be regularly revised to reflect any changes in the banking and regulatory environment in which the bank operates.

Whereas different banks may have codes of conduct with varying sections, the following, at a minimum, should be included in a bank's code of conduct:

- An introductory letter from the Board and senior management that sets the tone at the top and defines the importance of the code and the need for compliance by each member of the Board, senior management and employee in the bank;
- The bank's mission statement, vision, values, and guiding principles that reflect the bank's commitment to ethics, integrity, and quality;
- An ethical decision framework to assist employees in making the right choices and thinking of the consequences of their actions, and seeking help when unsure;
- A listing of the available resources for obtaining guidance, means to report issues anonymously, how to contact an ethics officer, and the reporting chain of command;

Case Study 2: Ensuring common values

To ensure that all its employees across the markets it operates in have aligned their values and interests with its approach to business, one of the banks interviewed has developed a code of ethics ("Code") which all employees are required to review and sign off on to confirm understanding. The Code, available on the bank's intranet, has the following objectives:

- To provide a collective statement of standards for personal and corporate behavior;
- To foster employee behavior that aligns with the bank's core values—Integrity, Accessibility, Mutual Respect and Continuous Learning;
- To ensure adherence to principles of professional behavior;
- To promote and maintain confidence in the banking profession;
- To resist and highlight improper or unprofessional conduct;
- To instill a sense of honesty, fairness, and decency in the conduct of banking business;
- To harmonize the concepts of profitability and social responsibility;
- To reinforce compliance with regulators' requirements;
- To enhance and sustain public confidence in the banking industry;
- To safeguard the cornerstones of the banking profession; and
- To respect the bank's rules of professional conduct.

The Code is a mandatory module for all staff orientation classes and is also accessible in the bank intranet to all staff. The bank in 2013 introduced a mandatory e-learning module which all bank staff are required to undertake on an annual basis to confirm and refresh their understanding of the Code.

It is reviewed alongside the Human Resources (HR) policy manual annually (where applicable). The Code, which was developed seven years ago by the HR team in liaison with the Legal and Compliance team, has been approved at the senior management level and by the Board of Directors and has benefited the bank in many ways, i.e., it is instrumental in instilling discipline and thus enhancing internal controls performance of the bank. It encourages ownership, accountability, compliance, confidentiality and ethical behavior.

The bank's Management Disciplinary Committee—which reports to the Board HR Committee—enforces the code of ethics by adjudicating any infringements by an employee and, depending on the severity, recommends an appropriate sanction, which could be a caution, warning, suspension or termination.

- A listing of any additional ethics and related resources, website and/or any supplementary policies and procedures and their location; and
- Examples of what constitutes acceptable and unacceptable behavior.

The code of conduct document should be availed to all members of the Board, senior management, and employees, and should encourage commitment to the application of the defined ethical principles in all business activities when making decisions. This should be implemented through requiring all employees and Board members to read and commit to the code of conduct or policy through their sign-offs.

2.2.2 RIGHT TONE AT THE TOP ON RISK MANAGEMENT

Checkpoint:

- ✓ Sufficient, sustained, and visible leadership on risk related issues
- ✓ Action and clear accountability toward managing risk
- ✓ Regular communication on risk management

The Board and senior management should set the tone on risk culture. If leadership makes risk management a priority and demonstrates it in their actions, then this will filter through to the rest of the bank.

To support the right tone at the top:

- There should be consistent, coherent, sustained and visible leadership in terms of how the Board and senior management act and expect the employees to behave and respond when dealing with risk.
- There should be regular and meaningful communication from the Board and senior management on matters or topics related to risk management, such as considering risks in decision making throughout the bank and creating an environment where there is constructive challenge on risk discussions and decisions.

2.2.3 COMMON UNDERSTANDING OF RISK MANAGEMENT TERMS

Checkpoint:

The Bank has:

- ✓ An enterprise-wide risk management policy
- ✓ Common definitions and categories of risk; and
- ✓ Regular risk awareness training

There should be a common understanding of the risk management framework across the bank. In this regard, banks should enact a policy document that establishes and guides a consistent, integrated approach to the identification, assessment and management of risk on an "enterprise-wide" basis.

The risk management policy document should outline, among other things:

- The definition of common risk management terms, such as "risk," "risk management," "risk appetite," "risk management framework," "risk impact," "risk factor," "risk prioritization" and "risk mitigation."
- Specific roles and responsibilities of individuals with regard to risk management within the bank. This includes roles of the Board, risk committees, senior management, management-level committees, business unit managers, risk management function, internal audit, and all employees.
- The process and key principles for determining the risk appetite, including reference to the documented risk appetite statement as approved by the Board and ongoing review.
- The bank's risk management framework and structure, including the role of the Chief Risk Officer (CRO) and risk division units.
- Risk categorization, which includes a common understanding of the various classifications of risks facing the bank such as strategic risks, credit risks, liquidity risks, market risks, operational risks, information and communication technology risks, reputational risks, compliance risks, and country and transfer risks. This would ensure relationships among the various risks in the different business units are uncovered.
- Risk assessment guidelines to evaluate the potential likelihood and impact to assist with the prioritization of risk treatment strategies.
- Risk awareness channels for employees, including regular and scheduled training on risk management and induction for new employees and Board members. This creates a clear and complete picture of the risk management processor program in the bank.

In addition to the above, the risk management policy should have the following sections:[13]

- Risk management and internal control objectives (governance);
- Statement of the attitude of the bank towards risk (risk strategy);
- Description of the risk aware culture or control environment;
- Level and nature of risk that is acceptable (risk appetite);
- Risk management bank and arrangements (risk architecture);
- Details of procedures for risk recognition and ranking (risk assessment);
- List of documentation for analyzing and reporting risk (risk protocols);
- Risk mitigation requirements and control mechanisms (risk response);
- Allocation of risk management roles and responsibilities;
- Criteria for monitoring and benchmarking of risks;
- Allocation of appropriate resources to risk management; and
- Risk activities and risk priorities for the coming year.

2.2.4 UNIVERSAL APPLICATION OF RISK MANAGEMENT PRINCIPLES

Checkpoint:

- ✓ Meeting agendas include risk discussions
- ✓ Risk objectives are quantifiable

All business activities of the bank from strategic planning to day-to-day operations should consider risk. Risk management discussions should be a standing agenda

13 The Association of Insurance and Risk Manager, *A structured approach to Enterprise Risk Management (ERM)*, 2010, p. 10.

Case Study 3: Consideration of risk management principles

In addition to defining a risk management framework that contains the definitions of key risk terms and their categorizations, a participating bank in this study further enhances the universal application of risk management principles through continuous discussion. Risk management is a standing agenda on the Board and Board subcommittee meetings as well as Management Operational Committee meetings.

The bank further ensures that its officials consider the risk implications of their decisions through risk assessments as one of the key steps in approval of new products and/or initiatives and through regular Risk and Control Self Assessments (RCSAs) and Key Control Risk Assessments (KCSAs).The business units provide information in the RCSA and KCSA templates provided by the Risk Management Division. Any new risks identified are discussed at the monthly Management Operational Risk Committee and mitigating actions are identified.

To further ensure that risk management principles are applied uniformly in the bank, risk management discussions are held at departmental meetings. With these practices, there has been a better and considerably active engagement between the business and risk functions thereby leading to a reduction of losses relative to business growth and day-to day operations.

item at all Board and senior management meetings. Risk management discussions should also be entrenched in all business decision-making meetings held by various business units.

Risks should be identified and measured in relation to the bank's risk assessment objectives. To ensure risk management principles are applied in all bank activities and decision-making, the risk objectives must be specific and quantifiable at various levels in the bank.

2.2.5 TIMELY, TRANSPARENT, AND HONEST COMMUNICATION ON RISKS

Communication is the continual, iterative process of providing, sharing, and obtaining necessary information. Internal communication is the means by which information is disseminated throughout the bank, flowing up, down, and across the entity. It enables employees to receive a clear message from the Board and senior management that risk management responsibilities must be taken seriously. External communication has two important uses: it enables inbound communication of relevant external information, and it provides information to external parties in response to requirements and expectations.[14]

Communication is an integral part of risk management and includes educating the bank's Board, senior management, and employees on the bank's risk management practices, collection of feedback, and constructive dialogue around the risks facing the bank. The bank's governance processes should provide for easily accessible and reliable communication channels that will ensure that internal stakeholders of the bank are encouraged to report new and emerging risks in their areas of operation and external stakeholders are updated on the bank's risk management efforts.

Effective communication enhances risk awareness in the bank across Board members, senior management, and employees at all levels. The bank can disseminate its policies and procedures through various internal communication channels such as notice boards, periodic bulletins, and the intranet so that risk awareness resonates across all levels of the bank. In a recent study undertaken by Ernst and Young,[15] 74 percent of the respondents indicated that they are enhancing communications and training programs to raise awareness of risk values and expectations.

The bank should establish mechanisms to internally communicate information necessary to support the proper functioning of its risk management framework. These mechanisms should ensure that:[16]

- Important components of the risk management framework are communicated appropriately;

14 Committee of Sponsoring Organizations of the Treadway Commission, *Executive Summary: Internal Control—Integrated Framework*, 2013, p. 5.

15 Ernst and Young, 2014 Risk management survey of major financial institutions "Shifting focus: Risk culture at the forefront of banking," 2014, p. 12.

16 Committee of Sponsoring Organizations of the Treadway Commission, *Executive Summary: Internal Control—Integrated Framework*, 2013, p. 7.

- Relevant information derived from risk management practices are available at appropriate levels and times; and
- Feedback channels are available for the internal stakeholders.

As the bank is required to communicate regularly with external stakeholders on its handling of various risks, the communication plan should involve:

- Engaging appropriate external stakeholders and ensuring an effective exchange of information;
- External reporting to ensure compliance with legal and regulatory requirements;
- Communicating with stakeholders in the event of a crisis.

Key questions that should be considered with regard to a bank's communication and awareness channels include:

- Has the bank taken into account different views on risk from various stakeholders, and relevant supervisory requirements?
- Have the bank's policies and procedures on risk-related activities been communicated in a timely manner to all employees?
- Is there a sense of the risk culture in the bank? Are risks and exceptions escalated through proper channels?

Good risk communication should have the following characteristics:

- **Completeness:** All the required information should be included in risk communication. This ensures that the recipients are able to make decisions as soon as they get the information.
- **Conciseness:** The risk communication should only include relevant information. The sender should focus on the message that he intends to pass across, and avoid unnecessary information that might confuse the recipient.
- **Correctness:** All risk communication should only include accurate facts to enable the recipients to gauge the importance of the required actions.
- **Credibility:** All communication should originate from people and/or offices in the bank with sufficient influence.
- **Communication in the bank should flow upward, downward, and across the bank** to enable the risk function to provide information to the various stakeholders and actively seek and act on the feedback provided.

To ensure effective communication, a bank could deploy the following tools:[17]

- **Charts and narratives of business objectives linked to risk tolerance levels:** These are simple explanations that show the bank's current risk profile in relation to its objectives.
- **Automated dashboards and detailed reports of key risk indicators:** A dashboard is a simple pictorial snapshot of the bank's major risks, the mitigation actions, and the risk owners. Dashboards are useful when updated regularly. The bank should therefore ensure that the dashboard has been cascaded from the Board to the senior management and operational management. Reports should be generated from the dashboard as and when required and appropriately distributed in a timely manner.
- **Flowcharts and maps of processes with key controls:** A flowchart is a pictorial representation of the bank's business processes. It is developed from the operational manual and identifies the key internal controls that the management has put in place. As flowcharts are easy to understand, the bank employees can contribute to the improvements of the various controls or processes.
- **Discussions and briefings on routine and special topics:** The risk management function should ensure that the bank regularly updates its stakeholders on its current risk profile. Operation units should be involved in the identification of mitigation actions on emerging risks.
- **Whistle-blower channels:** These are anonymous modes of communications that are made available for stakeholders to report any risks or illegal activities noted. To encourage use of the whistle-blower channels, the bank should communicate the anonymity safeguards to stakeholders. Investigations should be carried out on any reports received through such channels.

2.2.6 RISK MANAGEMENT RESPONSIBILITY—INDIVIDUALLY AND COLLECTIVELY

Checkpoint:

✓ Awareness of employees' roles in risk management

All employees should take personal responsibility, individually and/or collectively, for the management of risk in the business and should proactively seek to involve others when appropriate.

17 International Finance Corporation, *Standards on risk governance in financial institutions*, 2012, p. 14.

The risk management framework should codify roles and responsibilities of everyone in the bank with regard to risk management and provide clarity about responsibility. Although certain people will be charged with monitoring specific risks, everyone should ensure that risks are considered in all decisions within the realm of their duties and responsibilities.

To achieve this, the bank should establish risk committees (see Figure 2) at different levels of management.

A bank considering establishing a Board risk committee might consider the following key factors:[18]

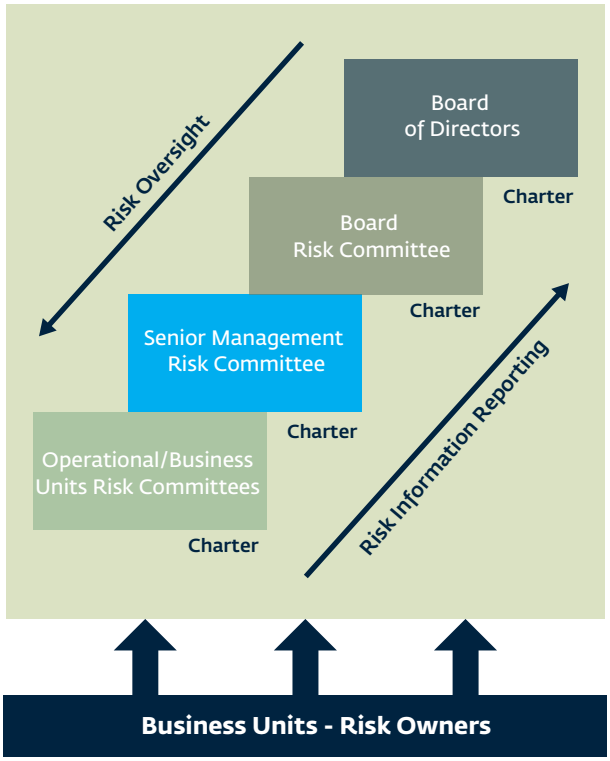
The needs of stakeholders. Whether or not the bank will be required by the regulator(s) to have a risk committee, the needs of the bank and its stakeholders should be considered. The Board should also assess the quality and comprehensiveness of the current risk governance and oversight structure, the risk environment, and the future needs of the bank. The composition and activities of the risk committee and its relationship with other Board committees could reflect the Board's assessment of these factors.

Alignment of risk governance with strategy. The Board should consider whether risk oversight and management are aligned with management's strategy. Banks vary in their business models, risk appetite, and approaches to risk management. A key consideration is that the Board, management and business units be aligned in their approach to risk and strategy—to promote risk taking for reward in the context of sound risk governance.

Oversight of the risk management infrastructure. The Board should consider whether the risk committee is responsible for overseeing the risk management infrastructure—the people, processes, and resources of the risk management program—or whether the audit committee or entire Board will oversee it. The CRO should have a dual reporting relationship to the risk committee, or Board, and the CEO.

Scope of risk committee responsibilities. The Board may need to decide whether the risk committee will be responsible for overseeing all risks, or whether other committees, such as the audit committee or the compensation committee, will be responsible for some. For example, oversight of risks associated with financial reporting may remain under the audit committee, while those associated with executive compensation plans might remain with the compensation committee. But because functional risks (such as tax or human resources risk) are often connected to operational or strategic risks, it is important to consider how the interconnectivity of risks is addressed. In any event, the Board will need to determine which committees will oversee which risks.

Figure 2: Illustrative risk management responsibilities



Adapted from Deloitte, *Improving Bank Board Governance: The bank board member's guide to risk management oversight.*

Communication among committees. The Board should consider how the committees will keep one another—and the Board itself—informed about risks and risk-oversight practices. Efficiency and effectiveness call for clearly defined responsibilities, communication channels, and handoff points.

In addition to the Board being in charge of risk management oversight, establishing other related committees allows for a more coordinated, integrated and focused approach to risk management. It enables the Board to:[19]

18 Deloitte, *Risk Committee Resource Guide for Boards*, 2012, p. 3.

19 Deloitte, *As risks rise, boards respond: A global view of risk committees*, 2014, p. 17.

- Assert and articulate its risk-related roles and responsibilities more clearly and forcefully;
- Establish its oversight of strategic risks, as well as the scope of its oversight of operational, financial, compliance, and other risks;
- Task specific Board members and other individuals with overseeing risk and interacting with the senior management and the CRO;
- Recruit Board members with greater risk governance and risk management experience and expertise. Keep the Board more fully informed regarding risks, risk exposures, and the risk management infrastructure;
- Elevate risk as a management and an enterprise-wide concern in day-to-day operations; and
- Improve advice provided to senior management regarding risk, response plans, and major decisions, such as mergers, acquisitions, and entry into new markets or new lines of business.

The charter for the committees tasked with risk management will describe the roles and responsibilities of overseeing the risk management framework. The committees should ensure that risk management responsibility is segmented, involves all employees, and that they clearly understand their risk management roles and responsibilities. In developing the Board Risk Committee charter, the following information should be included:[20]

- The risk oversight responsibilities of the committee and how it fulfills them;
- Who is responsible for oversight of management's risk committee; for example, whether it is the Board risk committee or the full Board (it is the full Board that is ultimately accountable and responsible for risk governance);
- Who is responsible for establishing the criteria for management's reporting to the Board about risk (the actual criteria need not be set in the charter, because it is expected to change as the bank and risks evolve);
- The composition of the Board risk committee and the qualifications of risk committee members (the committee should include a risk management expert, and it should be made up of a majority of independent Board members);
- The Board's or risk committee's responsibilities regarding the bank's risk appetite, risk tolerances, and utilization of the risk appetite;
- The Board's or risk committee's responsibility to oversee risk exposures and risk strategy for broadly defined risks, including, for example, credit, market, operational, compliance, legal, property, security, IT, and reputational risks;
- The risk committee's responsibility to oversee the identification, assessment, and monitoring of risk on an ongoing bank-wide or line of business basis;
- The reporting relationships between the Board risk committee and the CRO and the management risk committee;
- The risk committee's oversight of management's implementation of the risk management strategy; and
- Terms of service of risk committee members and the chair, with incumbents subject to reappointment; term limits (which may preclude members or chairs from having their terms renewed) may not be desirable because they may cause the loss of individuals in valued roles.

An illustrative risk committee charter has been included in Annex 3 to demonstrate how the above elements can be incorporated within a bank's governance documents.

2.2.7 EXPECTATIONS ON CHALLENGING DISCUSSIONS AROUND RISK MANAGEMENT

Checkpoint:

✓ People can comfortably discuss risk issues without fear of repercussions

All employees should have a working knowledge of the key risks facing the bank and more in-depth knowledge of the risks in their individual roles. To achieve this, the Board and senior management should create an enabling environment where employees freely engage in risk discussions in the execution of their duties.

All employees, at all levels, should be encouraged to discuss risk management with others, including authority figures. Potential risks noted during these conversations should be appropriately escalated to ensure that they are appropriately mitigated.

In a bank environment where employees are not free to discuss risk situations, major risks within the bank's critical functions may not be timely identified and mitigated. Employees who do not have sufficient understanding of the risks associated

20 Deloitte, *Risk Committee Resource Guide for Boards*, 2012, p. 7.

Case Study 4: Risk management responsibilities

A listed commercial bank offering a full range of corporate and retail banking services that participated in this study has identified risk champions across the business to help embed the "right" risk culture across the bank and ensure individual and collective ownership over risk management and reporting.This ensures that the risk champions have constant interactions with the business units they represent. The information collected by the risk champions is then reported to the Board on a quarterly basis through the Risk Function.

Risk champions are identified within the business unit based on their performance. They must have substantive knowledge of the business unit to be able to effectively guide the business unit on coordinating and reporting on risk management issues through the Risk Management department. The champions undergo regular formal risk management training from the Risk Management department and external consultants as appropriate to guide them in their role as risk champions.

Through the risk champions, the bank has been able to benefit from a more coordinated and focused approach to risk management. The business units with support from their risk champions and the risk management function are involved in developing the mitigating actions in their respective business units thus facilitating effective risk ownership in the Bank.

with the bank are likely to expose the bank to imprudent risk taking.

2.2.8 RISK REPORTING AND WHISTLE-BLOWING MECHANISMS

Checkpoint:

- ✓ Availability of whistle-blowing mechanisms such as reporting hotlines, ethics integrity lines, email address and or a web portal for reporting issues anonymously

Banks should have formal processes and reports for risk reporting to the Board, senior management, and other relevant stakeholders. The risk management framework should define such processes, reports, and performance standards for employees in preparing and reporting risk information.

Communication remains a challenge with 62 percent of the respondents in the 2013 Deloitte survey on Culture in Banking under the Microscope,[21] indicating that they believe that upward communication of concerns to management, or lack thereof, was a significant cultural problem. Twenty-six percent of the bankers interviewed in the same survey agreed that they had mechanisms on whistle-blowing. In other instances, the survey found that whistle-blowing channels were seen to focus more on form rather than substance, with indications that organizations are just going through the motions, with insufficient consequences when poor behaviors are identified.

A bank's failure to adequately provide for risk event reporting and whistle-blowing mechanisms could weaken its ability to identify and manage risks. Senior management's failure to recognize and address issues raised may lead to a significant impact on the bank's overall performance and reputation.

> "If you don't open up your information or mention anything that is negative, you are misleading yourself at the end of the day because you are not addressing properly the issues and you are wasting a very great opportunity to improve your culture. We want to be as transparent as possible to the outside stakeholders and then internally."
>
> —Matias Rodrigues Incite, Vice Chairman, Banco Santander[a]

a KPMG, *Expectations of Risk Management Outpacing Capabilities: It's time for action*, 2013, p. 20.

To support risk reporting and whistle-blowing mechanisms:

- The bank should have a formal process for reporting risk to the Board or a Board mandated committee—for example, the Board Audit Committee or the Board Risk Committee and other relevant key stakeholders such as the bank regulator.
- The bank should define a reporting matrix for escalating risk issues. Employees should have a clear understanding of the channels and processes, as well as rights and

21 Deloitte, *Culture in banking: Under the microscope*, 2013, p. 11.

protections, for raising risk issues, whether directly or anonymously.

- The bank should have an appropriate risk management toolkit for data collection and tracking of risks. This will ensure constant availability of data for objective quantification of the risks, which would advise the bank's approach to risk assessment.
- Whistle-blowing channels such as an anonymous reporting hotline, ethics, integrity lines, anonymous email address and/or a web portal for reporting issues anonymously should be put in place and their usage monitored.
- Whistle-blower issues should be duly acknowledged and investigated by senior, independent management who have sufficient authority to investigate and manage the issue.

To ensure the protection of whistle-blowers, the bank should ensure the following:[22]

- **Confidentiality of identity.** An employee reporting a serious irregularity in good faith should be guaranteed that his or her identity will be treated in confidence.
- **Mobility.** The bank should facilitate the redeployment of the concerned employee, if he or she wishes, to another department or function in order to safeguard himself or herself from possible hostile reactions from his or her immediate department or function.
- **Appraisal and promotion.** Care should be taken during staff appraisal and promotion procedures to ensure that the whistle-blower suffers no adverse consequences.
- **Penalties for those taking retaliatory action.** The Board, senior management, and the immediate supervisors should not use their positions to prevent employees for reporting any serious irregularities. Any form of retaliation undertaken as a result of whistle-blowing should be sanctioned.
- **Anonymity.** As the above procedures reduce the need and justification for anonymity, an employee should be encouraged to identify himself or herself to the bank to enable the bank apply the whistle-blower protective measures.

22 Adapted from the European Commission, *Communication to the Commission: Communication from Vice President Šefčovič to the Commission on Guidelines on Whistleblowing*, 2012, pp. 6–8.

2.3 RISK CULTURE MATURITY RATING SCALE

Table 2 presents criteria that can be used to assess a bank's maturity against each of the risk culture best practices. This scale represents three levels of maturity: "Below Standard," "Standard," and "Above Standard."

Table 2: Bank's maturity against each of the risk culture best practices

Component	Below Standard	Standard	Above Standard
Commonality of purpose, values, and ethics in the bank	There is no code of conduct that spells out the expected employee behaviors. Low ethical standards exist.	There is a code of conduct, but it is not strictly enforced. Ethical standards are established but not consistently applied or are more apparent in some business units than in others.	There is a code of conduct which is fully enforced. All employees are required to review the Code of Conduct and to sign off to acknowledge their understanding. There is regular assessment of the employees' understanding of the Code of Conduct. High ethical standards exist and are apparent in all business units.
Right tone at the top	The Board has not set the tone for managing risks, and the culture of risk awareness does not exist in the bank. Risk appetite has not been defined, and/or risk metrics are not included in performance metrics. The Board does not assess the risk culture of the bank and attitudes toward risk throughout the bank.	The Board sets the tone for managing risks and demonstrates a culture of risk awareness at the top level but it has not been embraced broadly. The Board has approved a risk appetite and the risk metrics are included in some employee's performance metrics. The Board infrequently assesses the risk culture of the bank and attitudes toward risk through a top-down approach.	The Board sets the tone for managing risks and establishes a culture of risk awareness, which is widely adopted and understood throughout the bank by ensuring the bank has an approved risk appetite and that risk metrics are included in performance metrics for all employees. The Board assesses the risk culture of the bank and attitudes toward risk throughout the bank through mechanisms, such as employee and vendor surveys, on an ongoing basis.
Common understanding of risk management terms	Risk has not been commonly defined throughout the bank. Risk is defined differently at different levels in the bank.	The bank has a common definition of risk, and it is communicated to the rest of the bank using a top-down approach.	The bank has a common definition of risk and a clearly articulated risk management strategy that addresses both value preservation and value creation and is used consistently throughout the bank.
Universal application of risk management principles	A few members of the senior management have limited consideration for risk as part of their core decision-making processes. There is limited participation and accountability of business units in overseeing the risk management program. There is a culture of unnecessary risk taking. Only some risks are considered in the decision-making process.	A few members of the senior management periodically request information from management when they consider the risk of action or inaction as part of their core decision-making processes. A few business units, e.g., finance, are primarily held responsible by management for overseeing the risk management program and provide updates to management. Only top management takes risks, as per the defined risk appetite of the bank. Top management considers a set of risks in the decision-making process	Appropriate senior members of the management staff systematically consider the risk of action or inaction as part of their core decision-making processes. Appropriate business units gather, analyze, aggregate, communicate, and report to the Board and management on the enterprise-wide risk management process on an ongoing basis. All employees follow risk management practices in effectively weighing their actions in the decision-making process, and there is a culture of involving risk experts in the decision-making process. Risks are taken as per the risk appetite of the bank and people are held personally accountable for managing risks.
Quality of information and communication channels	Minimal or no communication occurs in the bank on matters relating to enterprise risk management. The Board and other governing bodies lack transparency and visibility into the enterprise's risk management practices.	Communication on risk management occurs, but it is top-down. The Board and other governing bodies request and receive periodic updates into the bank's risk management practices.	There is consistent and effective communication within the bank flowing upward, downward, and across the bank as well as with external parties supporting the enterprise-wide risk management practices. The Board and governing bodies authorize the formation of an executive-level risk committee, with a composition, including representatives from all business units or departments, to have transparency and visibility into the enterprise-wide risk management practices.

Table 2: Bank's maturity against each of the risk culture best practices (continued)

Component	Below Standard	Standard	Above Standard
Risk management responsibility	There is a lack of individual or collective management of risks in the bank. Limited number of risk events that have high impact and high vulnerability are inconsistently reported.	Discrete roles, responsibility, and delegation of authority have been defined for a limited set of risks as a part of the governance structure. There is limited individual and collective risk management responsibilities being practiced in some sections/business units.	Well-defined and delineated roles, responsibility, and delegation of authority promote collaboration and coordination for developing and sustaining a governance structure and executing on the bank's risk management strategy. Individual and collective risk management responsibilities are practiced across all business units.
Discussion around risk management	People do not question decisions made by their superiors. Individuals yield to inappropriate pressure from others. There is inadequate challenge of excessive risk taking. There is reluctance to escalate risks appropriately.	People challenge others if they think they are not doing the right thing. Some people in the bank respond well to challenging discussions on risk management.	There is open and honest dialogue regarding risks. There is constructive response to challenges. People are confident when raising risk management concerns.
Risk reporting and whistle-blowing	Risks are minimally reported and monitored in the bank. The bank does not have a whistle-blowing mechanism.	Key risks are reported and monitored through separate evaluations by top management in the bank. Only risk events that have high impact and high vulnerability are reported. The bank has a whistle-blowing mechanism in place but investigations and sanctions are not consistently carried out and enforced.	All risks are reported and monitored holistically at the enterprise level. Attention is drawn to risk events other than those that have high impact and high vulnerability. Attention is drawn and resources made available proactively to address risk events other than those that have high impact and high vulnerability. Whistle-blowing mechanisms are in place, and management sees this as a useful tool in its risk management process.

Adapted from the Global Financial Service Industry (GFSI) Risk Transformation Toolkit, Deloitte Development LLP, May 2013.

2.4 CONCLUSION

Banks must strive to create a culture of risk awareness within their operating environment, having appreciated its importance and significance to the bank's ability to identify and manage risk effectively.

The right risk culture can provide banks with a competitive edge that is difficult for its rivals to emulate. It greatly influences the bank's risk management efforts as well as the achievement of the bank's vision, mission and objectives.

A bank's risk culture is not a stand-alone component but is intertwined and influenced by the bank's risk governance practices as well as the incentives programs in place.

Risk governance is linked inextricably to the bank's culture. For a bank to reap the benefits of effective risk management, the Board and senior management must show commitment to their risk governance responsibilities, which in turn influence the risk culture of a bank. In the next chapter, we explore the role risk governance plays in effective risk management, well as some recommended best practices.

3 Risk Governance in Banks

A bank that can understand risk holistically—that is, being aware of the full range of risks it confronts—can strategically use risk taking as a means to strengthen its competitive position and reduce adverse impacts from risk.

At a Glance

Recommended best practices in Risk Governance

- Risk governance structure
- Risk management framework
- Qualifications and experience
- Training and capacity building programs
- Board evaluation

3.1 INTRODUCTION

A bank has many stakeholders that include the Board, senior management, employees, regulatory authorities, customers, suppliers, other banks and lenders, and the community in which it operates. Effective interaction with these stakeholders requires a bank to have good corporate governance practices. These practices include the processes, customs, policies, procedures, laws, rules, and regulations, which enable the stakeholders to interact in a transparent and sustainable manner.

Risk governance focuses on applying the principles of sound corporate governance to the identification, management and communication of risk. It incorporates the principles of accountability, participation and transparency in establishing policies and structures to make and implement risk-related decisions.[23] A sound risk governance framework promotes clarity and understanding of the ways in which bank employees execute their responsibilities.

The bank should strive to manage the risks its faces holistically by adequately assessing and addressing risk from all perspectives and quarters; breaking through the organizational barriers that may obscure a view of the entirety of risks facing the bank; and systematically anticipating and preparing an integrated response to potentially significant risks. This also requires institutions to move away from the traditional "silo-based" approach to risk management. Holistic risk management is a concept about managing all the risks simultaneously and is all about accountability—that is, people taking responsibility for their actions. Holistic risk management involves a methodology where the various risk types that can affect a bank are considered holistically, rather than independently.[24]

To ensure this, the bank's risk governance should exhibit the following characteristics:[25]

23 Adapted from IFC, *Risk Taking: A Corporate Governance Perspective*, 2012, p. 11.

24 Adapted from "The Application of Holistic Risk Management in the Banking Industry," by J. Chibayambuya & D.J. Theron, University of Johannesburg, p. 5.

25 Deloitte, *The Risk Intelligent Enterprise: ERM done right*, 2006, p. 2.

- Risk management practices that encompass the entire business, creating connections between the so-called "silos" that often arise within large, mature, and/or diverse enterprises;
- Risk management strategies that address the full spectrum of risks, including industry-specific, operational, compliance, competitive, business continuity, and strategic, among others;
- Risk assessment processes that augment the conventional emphasis on probability by placing significant weight on vulnerability;
- Risk management approaches that do not solely consider single events, but also take into account risk scenarios and the interaction of multiple risks;
- Risk management practices that are infused into the corporate culture, so that strategy and decision-making evolve out of a risk-informed process, and not considering risk after decisions are taken; and
- Risk management philosophy that focuses not solely on risk avoidance, but also on risk taking as a means to value creation.

Good risk governance practices influence the effectiveness of risk management, seen as fundamental for a bank's success in the global business environment, and a basic expectation of stakeholders, regulators, analysts, depositors, and customers. Improving risk governance in banks requires starting at the top of the management "pyramid," where the Board and senior management establish the bank's risk appetite, policies, and limits.

Effective risk governance and oversight begins with a solid mutual understanding of the extent and nature of the Board's responsibilities as compared to those of senior management and other stakeholders. Whereas the Board is accountable for the oversight of risk governance, the senior management is responsible for implementing the policies and procedures through which risk governance is achieved within the bank. Board-level responsibilities include setting the expectations and standards, elevating risk as a priority, and initiating the communication and activities that constitute effective risk management.

Banks can achieve optimal risk governance practices through the establishment and implementation of a risk governance operating framework, as discussed below.

3.1.1 RISK GOVERNANCE OPERATING FRAMEWORK

A risk governance operating framework is a mechanism that the Board and senior management can use to translate the elements of the bank's governance framework and policies into practices, procedures and job responsibilities. It can assist the Board and senior management to organize the risk governance responsibilities such that there are no inconsistencies, overlaps, and gaps among the governance mechanisms.

The risk governance operating framework has four main components:[26]

- **Structure:** A clear comprehensive organizational structure defines reporting lines for decision-making, risk management, financial and regulatory reporting as well as crisis preparedness and response. It includes organizational design and reporting structure, committee structures and charters, and control and support function interdependencies.
- **Oversight responsibilities:** Oversight responsibilities define the Board's responsibilities, committee and management responsibilities, accountability matrices, and management hiring and firing authorities. The Board carries out this responsibility across the bank in areas such as business and risk strategy, financial soundness, and compliance.
- **Talent and culture:** This component enables the behaviors and activities required for effective risk governance by establishing compensation and incentive policies, promotion policies, performance measurement management, training, and leadership and talent development programs. These factors should reflect the bank's overall commitment to governance as well as principles of asset preservation and risk taking for rewards.
- **Infrastructure:** This comprises governance and risk oversight policies and procedures, reports, measures and metrics, management capabilities and the enabling information technology (IT) support.

The four major components of the framework have subcomponents (see Table 3) that describe the activities required to create an effective risk governance operating framework. These activities ensure that the bank defines and documents the processes, procedures, and reporting mechanisms required to operationalize the framework.

26 Deloitte, *Developing an effective governance operating model: A guide for financial services boards and management teams*, 2013, p. 6.

Table 3: Components of a risk governance operating framework[a]

Component	Subcomponents	Descriptions
Structure	• Board structure and charter • Board Committees structure and charters • Organizational structure and reporting lines • Controls and support functions' roles	• Outlines Board and management committees' structures, mandates, membership, and charters. • Establishes the design of the risk management framework. • Delineates organizational structure, reporting lines, and relationships. • Highlights the roles and independence of control and support functions from business owners.
Oversight responsibilities	• Board oversight responsibilities • Committee authorities and responsibilities • Management accountability and authority • Reporting and escalation	• Delineates Board and senior management approved policies, supporting delegation of authority including reporting and escalation. • Outlines the types of committees (both Board and senior management) and associated responsibilities. • Specifies functional accountabilities for the day-to-day management of business practices across the bank.
Talent and culture	• Leadership development and talent programs • Business and operating principles • Core beliefs and risk culture • Performance management and incentives	• Aligns risk governance with operating and business principles. • Articulates core belief and foundation for risk culture. • Highlights characteristics of risk culture. • Outlines leadership succession, assessment, and development responsibilities. • Aligns performance management, approach, measures and responsibilities to compensation and incentive plans.
Infrastructure	• Policies and procedures • Reporting and communication • Technology	• Establishes design and content of manual and associated procedures. • Outlines type and frequency of internal reporting and communication. • Aligns technology and tools to the communication systems required.

a Deloitte, *Developing an effective governance operating model: A guide for financial services boards and management teams*, 2013, p. 9.

3.2 BEST PRACTICES IN RISK GOVERNANCE

To improve a bank's risk management program, a number of best practices are recommended. While the risk governance operating framework provides for the governance structure, it is notable that the qualitative components of the governance framework, such as the Board and senior management oversight role; commonality of values and ethics as codified in the code of conduct; performance management; incentives plans and communication channels, greatly influence the bank's risk culture and are cross-cutting practices between establishing the right risk culture and effective risk governance. An effective risk governance operating framework would entail having:

- **Risk governance structure:** The bank should clearly define the roles and responsibilities of the Board, senior management, employees, internal and external auditors, and other stakeholders in its risk management program.
- **Risk management framework:** The bank should have a well-defined risk framework. This is a formal process for identifying, assessing, prioritizing, responding and mitigating major business risks across all its business units.
- **Qualifications and experience:** The bank should ensure that the people charged with risk oversight have the required skills, expertise, and authority.
- **Training and capacity building programs:** The bank should continuously train its Board, senior management, and employees on risk management practices and emerging standards and requirements.
- **Performance management:** The bank should constantly evaluate how well its Board, senior management, and employees are working toward the achievement of the bank's long-term objectives. The performance measures should include risk metrics.

3.2.1 RISK GOVERNANCE STRUCTURE

Checkpoint:

- ✓ Board oversight role
- ✓ Existence of the three lines of defense

A risk governance structure defines the roles of the stakeholders in risk management and the processes by which risk information is collected, aggregated, analyzed, and

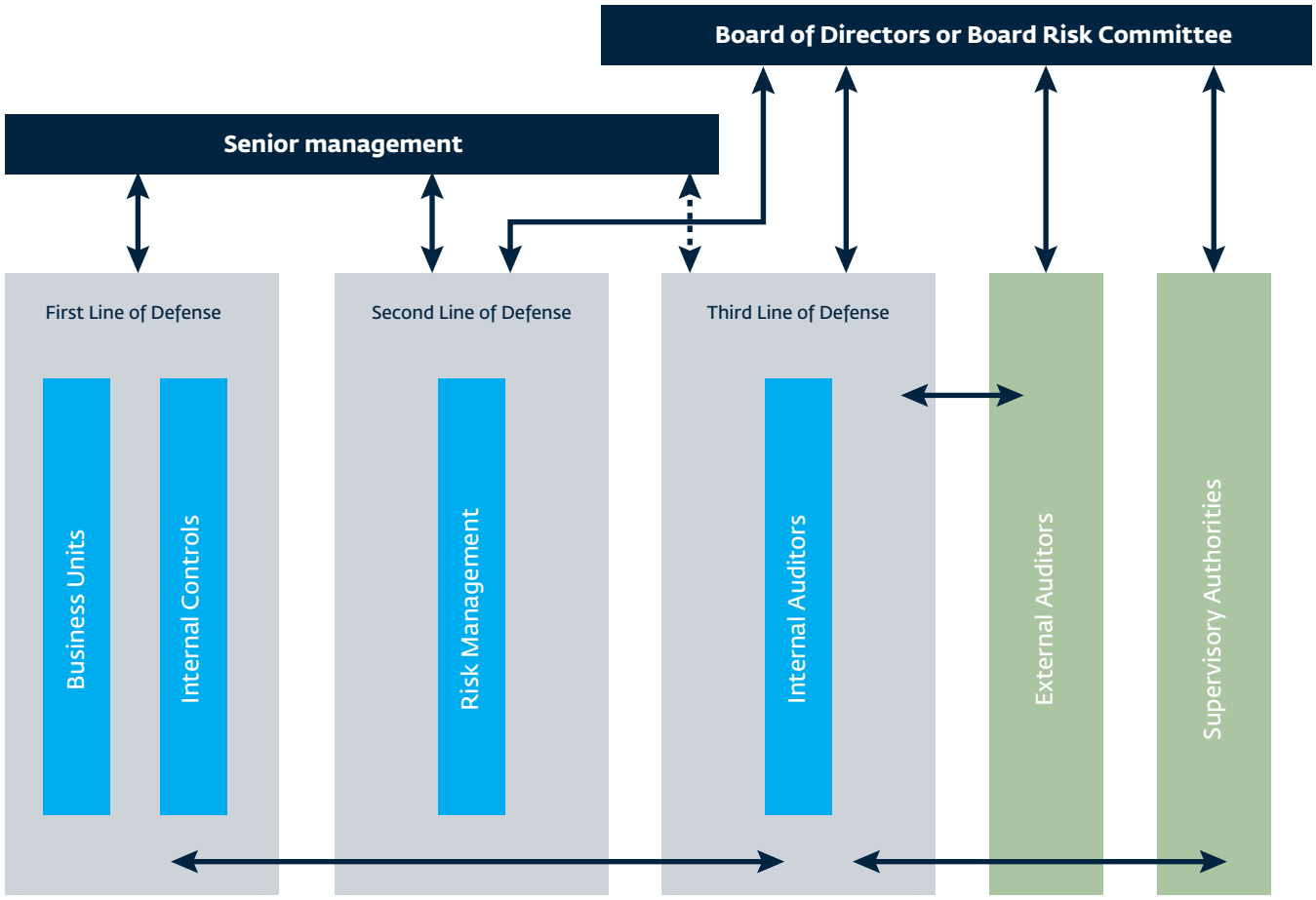
communicated to provide a sound basis for management decisions in the bank. The stakeholders include the Board, senior management, business units, risk management function, shareholders, internal and external auditors, creditors and debtors, regulatory bodies, and the general public. The bank should define an appropriate risk governance structure with input from the stakeholders that is consistent with the bank's business operations and applicable regulatory requirements. The risk governance structure should then be approved by the Board.

Effective risk governance should incorporate the three lines of defense, which are the operating management and internal controls, the risk management and compliance function, and the internal audit. The three lines of defense then interact with the Board or its subcommittees, senior management, and external bodies such as the external auditors and the supervisory authority to ensure effective enterprise-wide risk management in the bank.

The three lines of defense are expected to play complementary roles for sound risk management practices. However, the first line of defense can have a point of tension with the risk management and internal audit functions. The business units are remunerated for the business they generate for the bank and, in some cases, may view the activities of the subsequent lines of defense as a curtailment of their "main" objective. There is therefore a natural tension between value creation and value protection that may arise among the first line—i.e., business units whose primary objective is value creation, and the second and third lines whose primary objectives are related to value protection.

To ensure an effective risk governance structure, it is therefore important to enforce clear segregation of duties and independence in the reporting hierarchy for the three lines of defense. The second and third lines need to have enough influence, expertise, and independence in the bank to sufficiently challenge the risk takers and provide independent opinion and communication lines to the Board. In addition

Figure 3: Illustrative lines of defense



Adapted from the European Confederation of Institutes of Internal Auditors / Federation of European Risk Management Associations Guidance on the 8th EU Company Law Directive, article 41.

to this, the following elements would ensure an effective three lines of defense:[27]

- Each risk has a clear link to the responsible owner in the relevant line of defense;
- Clear roles and accountabilities are assigned across the three lines and documented in the form of charters to enable work activities. Where clear accountabilities are documented, there can be no wrong assumptions as to the responsibility for risk, controls and assurance;
- Each line has adequate skills to discharge its responsibilities. This is usually straightforward in the first line, but can be more complex in the second and third lines. Many monitoring and assurance functions do not contain deep knowledge of the business or industry, which provides a challenge in gaining the respect of the first line;
- Senior management and the Board receive one combined report showing the status for individual risks;
- Clear communication protocols are established between the three lines, risks, associated controls and assurance activities, defining the information to be exchanged and when;
- Risk owners are responsible for collating all information from across the lines for their risks and have specific points of contact in the other lines so as not to deal with multiple requests for information;
- A person or function is assigned responsibility for administering the model and overall coordination of reports; and
- A single technology system is used for all data input, and from which reports are generated for individual risks. At any point in time, the status of individual risks and associated controls assurance activities can be reviewed.

Further details on the roles and responsibilities of each of these three lines of defense in ensuring effective risk governance are provided in the following subsections.

3.2.1.1 *The Role of the Board of Directors and Board Subcommittees*

The Board has the ultimate responsibility for the bank's risk oversight. This includes:

- Knowing which risks the bank is willing to take in the pursuit of its objectives. This would be clearly stated in the risk appetite, which defines the maximum allowable loss by the type of risk and overall risk for the bank.
- Understanding the bank's risk profile. This includes the risks the bank faces, their potential impact, and the classifications of such risks.
- Keeping track of the compliance obligations of the bank, including the ones based on regulatory requirements and the ever-evolving industry expectations. The Board should ensure that it initiates efforts from its level, and that such efforts are cascaded throughout the bank to ensure relevant requirements are met.
- Determine that the bank's risk management infrastructure is consistent with the complexity of its business, the risks it faces, and all applicable laws, regulations and industry requirements.

When defining the roles and responsibilities for risk oversight, the Board should be clear about which committees are charged with oversight for which specific risks. Further to the guidance provided in Chapter 2.2.6 of this handbook on factors to take into account when establishing a Board risk committee, the Board may establish a Board risk committee that should be charged with:[28]

- **Overseeing the risk management infrastructure.** The full Board may oversee the organization's risk management infrastructure, or this oversight responsibility can be delegated to the Board risk committee, rather than to the audit committee;
- **Addressing risk and strategy simultaneously.** The Board risk committee should address risk management and governance when strategies for growth and value creation are being created and management decisions are being made. The purpose of this responsibility is to promote risk taking for reward in the context for practicing sound risk governance;
- **Assisting with risk appetite and tolerance.** The Board risk committee can assist , establish, communicate, and monitor the risk culture, risk appetite, risk tolerances, and risk utilization of the bank at the enterprise and business units;
- **Monitoring risks.** The Board risk committee should assist in assessing and monitoring the bank's compliance with the risk limit structure and effective remediation of

27 Ernst & Young, *Maximizing value from your lines of defense: A pragmatic approach to establishing and optimizing your LOD model*, 2013, pp. 6-7.

28 Deloitte, *Risk Committee Resource Guide for Boards*, 2012, pp. 11-12.

noncompliance on an ongoing and enterprise-wide basis. For the risk committee, this responsibility extends to all risks, or at least to all risks not monitored by the audit, compensation, or other Board-level committees. In cases of risks monitored by other Board committees, the Board risk committee should be made aware of ongoing risks.

- **Overseeing risk exposures.** The Board risk committee should consider the full range of risks and potential interactions among risks, including risk concentrations, escalating and de-escalating risks, contingent risks, and inherent and residual risk;
- **Advising the Board on risk strategy.** The Board creates the risk committee to serve as a repository of information and expertise on risk and to advise the Board on risk strategy. Thus, the Board risk committee can help inform the Board of risk exposures and advise the Board on future risk strategy;
- **Approving management risk committee charters.** Management may establish risk committees not only at the enterprise level, but also in some cases at business unit levels. The Board risk committee may consider and approve the charters of any such management risk committees;
- **Overseeing the Chief Risk Officer (CRO).** Like the Chief Audit Executive's (CAE) relationship with the audit committee, the Board or its risk committee should hire, evaluate, and determine the compensation of the CRO. The Board and the risk committee should consider how they might maintain ongoing communication with the CRO and the risk management function, including separate sessions with the CRO. In addition to having the CRO report directly to the Board or the risk committee, the risk committee can help ensure that the CRO has the seniority, authority, and resources to oversee risk in the enterprise. The Board can also support the CRO through consistent communications and actions regarding the bank's approach to risk and risk management; and
- **Consulting with external experts.** The Board risk committee should consider having access to external expert advice regarding risk and risk governance and management in the form of meetings, presentations, verbal or written briefings, or assignments commissioned by it. The areas to cover could include the risk environment, regulatory developments, leading practices, or any other items the Board or committee specifies. In some cases, the Board risk committee may seek external Board education regarding risk management or regulatory matters. In other cases, the Board risk committee may engage a consultant for a particular assessment or other efforts best commissioned at the Board level.

Case Study 5: Board level committees

One of the banks interviewed indicated having established a Board Integrated Risk Management Committee (BIRMC) and a Board Audit Review Committee (BARC) through which the Board maintained oversight of risk management activities at the bank. Through these committees, the Board fulfils its responsibilities of approving a risk management strategy for the bank, articulating the bank's risk appetite, establishing the risk governance structure, reviewing significant risk issues highlighted by its committees, reporting to stakeholders on risk management of the bank, and approving public disclosures.

The mandate of the BIRMC includes ensuring that the bank has a comprehensive risk management framework; assessing the effectiveness of the bank's risk management systems and monitoring risks through appropriate risk indicators and management information. The BIRMC ensures compliance with laws, regulations, regulatory guidelines, internal controls, and bank policies, and updates the Board on the bank's risk exposure.

The functions of the BARC include: making recommendations on matters in connection with the appointment, fee negotiation, resignation and dismissal of the external auditor of the Bank; discussing issues arising from the interim and final audits, and any matters the external auditor may so wish. The BARC also reviews the adequacy of the internal audit programs and results of the internal audit process and ensures that appropriate actions are taken on the recommendations of the internal audit department. As a champion of whistle-blowing, the BARC ensures that mechanisms are available for employees to report on possible improprieties in financial reporting, internal controls or any other matters and a fair and independent investigation of these reports.

The committees meet on a quarterly basis and decisions made at these meetings are enforced via the Risk Management Division of the bank who also submit quarterly reports to the Board.

3.2.1.2 The Role of Senior Management

Whereas the Board has the overall responsibility for risk management practices, the senior management is tasked with providing the correct infrastructure and processes for risk management and the appropriate tools to employees for effective execution.

As part of senior management's role in risk management, the responsibility for the day-to-day risk management function should be assigned to an officer at a senior level, in most cases a Chief Risk Officer (CRO) or equivalent, who should have sufficient seniority, authority, voice, and is independent from business line decisions and management.[29] This is to ensure that the CRO has the capacity/ability to influence key decision makers in the bank. Whereas the independence of the CRO from operational management is recommended, there should be sufficient interaction between the CRO and the operational management to ensure that the CRO and all risk managers have sufficient risk information from the business.[30] See Annex 4 for illustrative terms of reference of a CRO.

3.2.1.3 First Line of Defense: The Role of Business Units

The first line of defense is composed of the business unit (operational) managers, as they own the processes of the bank. As the first line of defense, operational managers own risks and therefore have the primary responsibility for establishing controls to manage the identified risks. They are also responsible for implementing corrective actions to address process and control deficiencies.

They are charged with owning and managing the risks that are in their departments.

The business units are charged with:

- Identifying and assessing risks;
- Implementing procedures and controls/limits consistent with the bank's risk appetite and policies;
- Responding to and mitigating risks; and
- Monitoring risks and providing reports to the risk management function, senior management and the Board.

The bank establishes internal controls, which are systems and procedures to ensure that its goals and objectives are achieved by ensuring that all the processes are correctly authorized, valued, classified, and recorded correctly and in a timely manner. They are implemented to ensure the bank's policies are being followed and its objectives are achieved.

The business units are responsible for maintaining effective internal controls and ensuring that risk and control procedures are duly executed on a daily basis. The business units identify, assess, control and mitigate risks, guide and implement the internal policies, procedures, and processes, while ensuring their activities are consistent with the bank's goal and objectives. The business units should have a tiered structure to enables middle-level management design and implement detailed procedures that would supervise execution of the bank's procedure by the employees. The business units serve as the first line of defense as controls are inbuilt in the bank's systems and procedures. There should be sufficient managerial control to ensure compliance and highlight any control breakdowns, inadequate processes, and unexpected events.[31]

3.2.1.4 Second Line of Defense: The Role of the Risk Management Function

The risk management function is responsible for the bank's risk management framework across the entire organization, ensuring that the bank's risk meets the desired risk profile as approved by the Board. The risk management function is responsible for identifying, measuring, monitoring, recommending strategies to control or mitigate risks, and reporting on risk exposures.

The risk management function should facilitate and monitor the implementation of an effective system of controls by operational management and guide the various operations of the business units in identifying the targeted and emerging risks. The function should act as a reporting and monitoring channel for risk-related information throughout the bank.

As the second line of defense,[32] the risk management function:

- Is independent of business lines (i.e., is not involved in revenue generation) and reports to the CRO;

29 Basel Committee on Banking Supervision, *Principles for enhancing corporate governance,* 2010, p. 18.

30 Ibid.

31 Institute of Internal Auditors, *IIA Position Paper: The three lines of defense in effective risk management and control,* 2013, p.3.

32 Financial Stability Board, *Thematic review on Risk Governance: Peer Review Report,* 2013, pp. 32–33.

- Has authority to influence decisions that affect the firm's risk exposures;
- Is responsible for establishing and periodically reviewing the enterprise risk governance framework, which incorporates the risk appetite framework (RAF), risk appetite statement (RAS), and risk limits:
- Has access to relevant affiliates, subsidiaries, and concise and complete risk information on a consolidated basis; risk-bearing affiliates and subsidiaries are captured by the enterprise-wide risk management system and are a part of the overall risk governance framework;
- Provides risk information to the Board and senior management that is accurate and reliable and is periodically reviewed by a third party (internal audit) to ensure completeness and integrity;
- Conducts stress tests (including reverse stress tests) periodically and by demand. Stress test programs and results (enterprise-wide stress tests, risk categories and stress test metrics) are adequately reviewed and updated to the Board or risk committee. Where stress limits are breached or unexpected losses are incurred, proposed management actions are discussed by the Board or risk committee. Results of stress tests are incorporated in the review of budgets, in the RAF and Internal Capital Adequacy Assessment Process (ICAAP), and in the establishment of contingency plans against stressed conditions.
- Is headed by a CRO who has the organizational stature, skill set, authority, and character needed to oversee and monitor the bank's risk management and to ensure that key management and Board members are apprised of the bank's risk profile and relevant risk issues on a timely and regular basis. The CRO should have a direct reporting line to the CEO and a distinct role from other executive functions and business line responsibilities as well as a direct reporting line to the Board and/or risk committee. In addition to this, the CRO:[33]
  - » Meets periodically with the Board and risk committee without executive directors or senior management present;
  - » Is appointed and dismissed with input or approval from the risk committee or the Board, and such appointments and dismissals are disclosed publicly;
  - » Is independent of business lines and has the appropriate stature in the firm, as his/her performance, compensation and budget is reviewed and approved by the risk committee;
  - » Is responsible for ensuring that the risk management function is adequately resourced, taking into account the complexity and risks of the firm as well as its RAF and strategic business plans;
  - » Is actively involved in key decision-making processes from a risk perspective (e.g., review of the business strategy / strategic planning, new product approvals, stress testing, recovery and resolution planning, mergers and acquisitions, funding and liquidity management planning) and can challenge management's decisions and recommendations; and
  - » Is involved in the setting of risk-related performance indicators for business units, senior management, and employees.

The second line of defense should also incorporate a compliance function, which ensures that the bank complies with institutional policies and procedures, standards for market conduct, internal controls, laws, rules and regulations. As banks operate within an environment that is highly regulated by a number of complex laws, rules, and regulations, a compliance function ensures that the bank is operating within the required legal and regulatory framework and thereby helping to reduce systemic vulnerabilities and financial crimes. In addition to this, compliance has become a Board level concern due to various factors:

- Banks are being held to higher standards of evidence of compliance;
- The compliance function itself is now subject to compliance;
- Whistle-blower channels may increase the chances of noncompliance being reported to the regulatory bodies;
- Penalties for compliance failures have become more severe, putting Boards and senior management at greater personal risks; and
- Shareholders, lenders, rating agencies, customers, suppliers, the media, and the general public care about compliance and are informed about it.

Compliance regulations (that include legislation, rules and standards issued by legislators and supervisors, market conventions, codes of practice promoted by industry associations, and codes of conduct applicable to the Board, senior management, and employees) that are country-specific, would cover matters such as observing the

33 Ibid., pp. 31–32.

proper standard of market conduct, managing conflicts of interest, fair treatment of customers, prevention of money laundering, and/or dealing with designated terror groups or individuals. In some countries, the regulators require that the designated compliance officer report to them on specific issues such as suspected cases of money laundering.

The compliance function should assist the senior management in managing compliance risks by: keeping them informed of emerging compliance issues and any new developments; educating staff on compliance issues; and establishing guidance to staff through policies, procedures and other documents such as guidelines. To guarantee an effective comprehensive function, the bank should also ensure the following:[34]

- The bank's Board oversees the management of the bank's compliance risk. It should approve the compliance policy;
- The bank's senior management is responsible for the effective management of the bank's compliance risk. The senior management should therefore establish an effective compliance function within the bank. The senior management should also be responsible for communicating the compliance policy and periodic reporting to the Board on the management of the bank's compliance risks;

34 Basel Committee on Banking Supervision, *Compliance and the compliance function in banks*, 2005 pp. 7–16.

Case Study 6: Regulator guidelines on the risk management and compliance functions—East Africa

One of the regulators in East Africa with over 44 banks under its jurisdiction recently issued updated risk management guidelines which require that banks and banking groups must have comprehensive risk management processes. A bank is required to have a comprehensive risk management function tailored to its needs and circumstances under which it operates and supervises the bank's overall riskmanagement.

The function should be independent from those who take or accept risks on behalf of the institution and should report directly to the Board Risk Management Committee. The risk management function is charged with:

- Identifying current and emerging risks;
- Developing risk assessment and measurement systems;
- Establishing policies, practices and other control mechanisms to manage risks;
- Developing risk tolerance limits for senior management and Board approval;
- Monitoring positions against approved risk tolerance limits; and
- Reporting results of risk monitoring to senior management and the Board.

The regulator has also issued guidelines on compliance risk. Compliance risk is defined as the risk of legal or regulatory sanctions, financial loss, or loss to reputation an institution may suffer as a result of its failure to comply with all applicable laws, guidelines, code of conduct and standards of good practice. The guidelines require the establishment of a compliance function. This should be an independent function which facilitates efforts to comply with legal and regulatory requirements by tracking and documenting compliance. The function should be sufficiently resourced and its responsibilities should be clearly specified.

Licensed institutions are required to organize their compliance function and set priorities for the management of their compliance risk in a way that is consistent with their own risk management strategy and structures. Some institutions may wish to organize their compliance function within their operational risk management function, as there is a close relationship between compliance risk and certain aspects of operational risk. Others may prefer to have separate compliance and operational risk functions, but establish mechanisms requiring close cooperation between the two functions on compliance matters.

The function should report independently to the Board, or committee of the Board, that identifies, assesses, advises, monitors and reports on the institution's compliance risk.

A bank that is licensed by the regulator to operate should therefore include compliance risk as part of its risk management processes and risks of non-compliance identified, assessed, and managed as part of overall risk management.

Case Study 7: The role of the risk function

To focus on the different risks facing the bank, one of the studied banks has established specialized units within the risk management department. The bank's risk department is responsible for monitoring and reporting on credit, market, and operational risks. The department has the following units:

- The credit risk management unit is divided to focus on the bank's three target markets—large companies, SMEs and retail customers. It performs analyses of the credit files before submission to the appropriate credit committees. Its other major roles include development of assessment tools and risk management, and internal regulatory reporting on credit risk performance;
- The market risk management unit's roles include monitoring bank counterparties, active contribution to the Asset and Liability Management (ALM) risk perspective, and monitoring the activities of the bank's exchange room. The assets and liabilities management unit assesses the bank's liquidity and interest rate risks to ensure adequate cover of its exposure to banking risks in line with recommendations of the Basel Committee for Banking Supervision; and
- The operational risk management unit's roles include outlining the framework for dealing with operational risks, collection of incidences and losses, and calculation of capital requirements.

The specialist units were established in the risk management department as part of the bank's quest to provide innovative and convenient banking services for the benefit of its stakeholders. This has benefited the bank by minimizing losses, protecting its revenues and providing sustainable business through a more thorough and in-depth risk monitoring and reporting process.

- The compliance function should be sufficiently independent and have sufficient resources to carry out its mandate effectively;
- The activities of the compliance function should be subject to periodic review by the internal audit function; and
- As the compliance function is an integral part of the bank's risk management program, if specific tasks are outsourced, the senior management should ensure sufficient oversight of the outsourced tasks.

3.2.1.5 Third Line of Defense: The Role of Internal Audit

In a risk governance structure, the internal audit function is charged with providing the senior management and the Board with assurance that internal controls are operating as intended, providing insights for improving the controls, processes, and procedures, and providing an objective view of the overall bank operations. The bank should establish and maintain an independent, adequately funded, and competent internal audit function, which acts according to international standards for the practice of internal auditing guided by associations such as the Institute of Internal Auditors (IIA).

The Chief Audit Executive (CAE) or equivalent should have a functional reporting line directly to the Board, through the Board Audit Committee, where this exists. The internal audit function supports the risk management practices in the bank by:[35]

- Reporting audit findings, significant issues, and the status of remedial action directly to the Board or audit committee on a regular basis;
- Providing an overall opinion on the design and effectiveness of the risk governance framework to the audit committee on an annual basis;
- Providing qualitative assessments of risks and controls. as opposed to evaluating compliance with policies and procedures;
- Assessing whether business and risk management units are operating according to the RAF; providing feedback on how the firm's risk governance framework and RAF compare to industry guidance and better practices as a means of influencing their evolution;
- Providing input to risk assessments and feedback on internal controls during the design and implementation processes; escalating issues and concerns identified in the course of audit work or through internal whistle-blowing, complaint, or other processes and situations where appropriate remedial action is not being implemented in a timely manner; and
- Being aware of industry trends and best practices.

35 Financial Stability Board, *Thematic Review on Risk Governance: Peer Review Report*, 2013, pp. 33–34.

The Board and/or audit committee should fully support the CAE and internal audit function by ensuring that the CAE:[36]

- Is organizationally independent from business lines and support functions and has unfettered access to the audit committee;
- Meets regularly with audit committee members outside of management's presence;
- Is appointed and dismissed with the approval of the audit committee (or chair of that committee);
- Has his/her performance, compensation, and budget reviewed and approved by the audit committee;
- Has the organizational stature, talent, and character needed to provide a reliable independent assessment of the firm's risk governance framework and internal controls and not be unduly influenced by the CEO and other members of management;
- Has the resources (people and systems) needed to effectively carry out the responsibilities of internal audit; and
- Provides regular reports to the Board or audit committee which summarize the results of internal audit's work, including overall conclusions or ratings, key findings, material risk/issues, and follow-up of management's resolution of identified issues.

> "Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes."
>
> —Institute of Internal Auditors

There should be synergy and cooperation between the bank's internal and external auditors to ensure a collaborative and productive relationship. External auditors could leverage on the internal auditor's activities and results to ensure efficient overall audit coverage for the bank.

The CAE must ensure that the bank has a quality assurance and improvement program of the internal audit function as prescribed by the Practicing Standards of the Institute of Internal Auditors. The program should evaluate the internal audit function's conformance with the standards of internal audit, and upholding of the principles of the IIA's Code of Ethics, including integrity, objectivity, confidentiality, and competence of the employees in the internal audit function. A quality assurance and improvement program enables the bank to ensure that its internal audit function complies with IIA standards, is adequately resourced, and has an appropriate reporting structure. It also ensures that the internal audit function becomes a reliable source of information on the bank's internal control environment and supports the overall objectives it was set up to achieve.

There should be both internal assessment and external assessment of the internal audit function. Internal assessment could be through ongoing monitoring of the performance of the internal audit function or through periodic self-assessments. External assessments should be undertaken at least once every 5 years.

As a means of further enforcing good governance, the results of the quality assessment of the internal audit function should be communicated to the Board and senior management. This should include any opportunities for improvement of the function and the impact of any non-conformance with the standards of internal auditing.

3.2.1.6 The Role of External Auditors

Traditionally, external auditors provide reasonable assurance to the bank's stakeholders that the financial statements are free from material misstatements. They do this by expressing an opinion on the bank's financial statements, focusing on whether proper books of account have been kept and maintained by the bank and whether the financial statements presented give a "true and fair view" of the financial affairs of the bank. The external auditor's opinion also indicates whether the bank's financial statements are in conformity with the accounting standards adopted by the bank, such as International Financial Reporting Standards (IFRS), in addition to adherence to the relevant Banking Act and the attendant regulations issued by the country's bank regulator.

On the basis of the opinion on the financial statements, as provided by the external auditors, the audited financial statements are then relied upon by the bank's stakeholders,

36 Ibid., p. 33.

who include the shareholders, investors, rating authorities, regulatory bodies such as the country's tax authorities, banking regulators, and securities regulators (if listed or issuing publicly traded debt instruments), in addition to the general public.

To form an opinion on the financial statements, the external auditors must gather appropriate and sufficient audit evidence and undertake audit procedures to review the bank's material account balances such as loans and advances and investments. They do this by gaining an understanding of the bank's operations and evaluating the bank's internal controls system to the extent that it addresses significant risks in the operations.

The external auditors also focus on adherence to risk management guidelines set by the bank regulator. They do this by reviewing the adequacy of the bank's policies and procedures on risk management (credit, liquidity, market, and operational risks) when compared to best practice and the regulator's guidelines. The external auditors test the extent of the implementation of the risk management guidelines while testing the bank's transactions and system of internal controls.

Although limited by scope, the external auditor offers an extra line of defense by providing independent assurance on the operating effectiveness of the system of internal controls to the bank's stakeholders. In addition to offering recommendations to the bank's management for improving the bank's processes, systems, and internal controls, external auditors address any other area(s) identified by the Board, that present(s) a significant financial reporting risk to the bank.

3.2.1.7 The Role of Supervisory Authorities

Bank regulatory agencies issue specific regulations and guidelines governing the operations, activities, and acquisitions of banks, with regulation and supervision playing complementary roles. Supervisory roles involve the monitoring, inspecting, and examining of banks to assess their compliance with the relevant laws, regulations, and supervisory directives.

Supervisory authorities issue guidelines on matters such as appointment of Board members; required cash reserve ratios, and minimum disclosure requirements, and as such they help a bank in shaping its internal control environment and the risk governance structure. The supervisory authorities in different countries are taking a more proactive approach and are adopting the Basel Committee guidelines in prescribing rules and regulations for the banks under their jurisdiction. In addition, in some emerging market countries, regulatory authorities have prescribed minimum standards for internal controls, risk management structure, risk management programs, maximum risk exposures, internal audit and external audit programs.

3.2.2 RISK MANAGEMENT FRAMEWORK

Checkpoint:

- ✓ Risk appetite statement
- ✓ A risk management toolkit
- ✓ ICAAP

A risk management framework is a formal process for identifying, assessing, and prioritizing major business risks across the bank. A risk management framework enhances the bank's value as its management strikes a balance between growth and related risk, thereby deploying resources efficiently and effectively. It assists the bank in:

- Addressing the relevant risks the bank faces in areas such as its strategy, planning, operations, finance, and governance;
- Acknowledging the risk management needs of specific business units and across the bank;
- Considering the causes of and interaction among various risks and the potential impact of multiple concurrent threats or events;
- Creating a common language for defining risks and developing a risk culture;
- Viewing risk taking as a way to achieve the bank's objectives rather than avoiding risks; and
- Employing risk-based methods in decision making, especially when deploying the bank's resources.

3.2.2.1 Components of an Enterprise Risk Management Framework

The Enterprise Risk Management (ERM) framework components in Figure 4 (page 35), based on the COSO framework, are recommended for effective risk governance.

The different players in the three lines of defense described in the previous section (3.2.1.2 to 3.2.1.6) are responsible for particular components of the risk management framework.

Case Study 8: Recommendations by the Monetary Authority of Singapore on corporate governance

In East Asia, the Monetary Authority of Singapore has the following as part of the corporate governance guidelines for financial institutions:

Independent directors should make up at least one third of the Board. There is a division of duties between the Chairman and the CEO. The Board should have a Nomination Committee that makes recommendations on:

- The review of Board succession plans for directors, in particular, the Chairman, and for the CEO;
- The development of a process for evaluation of the performance of the Board, its Board committees and directors;
- The review of training and professional development programs for the Board; and
- The appointment and re-appointment of directors (including alternate directors, if applicable)

The Board is responsible for the governance of risk and may establish a separate Board risk committee. The Board should ensure that the management maintains a sound system of risk management and internal controls to safeguard shareholders' interests and the bank's assets, and should determine the nature and extent of the significant risks which the Board is willing to take in achieving its strategic objectives. The Board should determine the bank's levels of risk tolerance and risk policies, and oversee management in the design, implementation and monitoring of the risk management and internal control (including financial, operational, compliance and information technology control) systems. The bank's risk management and internal control systems should be reviewed at least annually by the Board and a comment included in the bank's annual report as to whether the CEO or Chief Finance Officer (CFO) assured the Board on the effectiveness of the bank's risk management and internal control systems.The Board should also approve the appointment, remuneration, resignation, or dismissal of the CRO. The Board or the Board risk committee should have influence over the performance assessment and succession planning of the CRO.

The Board should establish an Audit Committee comprised of at least three directors with a majority of non-executive directors and an independent chairman. Its duties include:

- Reviewing the significant financial reporting issues and judgments so as to ensure the integrity of the financial statements of the company and any announcements relating to the company's financial performance;
- Reviewing and reporting to the Board at least annually the adequacy and effectiveness of the bank's internal controls, including financial, operational, compliance and information technology controls (such review can be carried out internally or with the assistance of any competent third parties);
- Reviewing the effectiveness of the bank's internal audit function;
- Reviewing the scope and results of the external audit, and the independence and objectivity of the external auditors; and
- Making recommendations to the Board on the proposals to the shareholders on the appointment, re-appointment and removal of the external auditors, and approving the remuneration and terms of engagement of the external auditors.

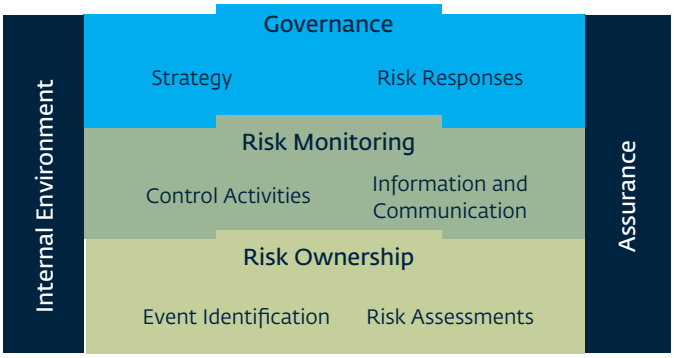
The bank should establish an effective internal audit function that is adequately resourced and independent of the activities it audits. The head of the internal audit should report functionally to the Chairman of the Audit Committee and administratively to the CEO. The adequacy and effectiveness of the internal audit function should be reviewed, at least annually, by the Audit Committee

The Board should also establish a Remuneration Committee, comprising at least three non-executive directors and an independent chairman. The Committee should review and recommend to the Board the remunerations for the Board and key management personnel (the key management personnel include the CEO and other persons having authority and responsibility for planning, directing, and controlling the activities of the bank). Lastly, the Committee should also seek the Board Risk Committee's views to ensure that the remuneration practices do not create incentives for excessive or inappropriate risk-taking behavior.The remuneration should take account of the risk policies of the bank, be symmetric with risk outcomes, and be sensitive to the time horizon of risks. Annually, the bank should also name and disclose the remuneration of the directors, CEO, and at least five key management personnel. The disclosure should include the fixed salary, incentive pay, benefits in kind, stock options granted, share-based incentives and awards, and other long-term incentives.

The components of the risk management framework and their responsibilities in this are described as follows:

- **Internal environment:** The internal environment encompasses the elements of the bank's risk culture. It takes into account the risk management tone, and sets the basis for how risk is viewed and addressed by the bank's employees. It includes the bank's risk management philosophy and risk appetite, integrity and ethical values, and the environment in which it operates. The risk appetite component is discussed in detail in section 3.2.2.2.

Figure 4: Components of a risk management framework which supports risk governance



Case Study 9: Three lines of defense to support the risk governance structure

To implement a robust risk management program, one of the interviewed banks has defined a governance structure based on the three lines of defense model. The bank has clearly defined roles for the Board, the internal audit and risk management functions, and the business units.

The Board is charged with risk oversight and determination of the bank's risk appetite and reviews the risk appetite appropriate to the bank's growth strategy. The Board has delegated its risk oversight responsibilities to committees that include the Board Audit Committee (BAC), Board Risk Management Committee (BRMC), Board Credit Committee (BCC), Information and Communication Technology (ITC) Committee, and the Assets and Liabilities Committee (ALCO).

The BAC is responsible for ensuring that the Bank's financial reporting is transparent by reviewing the effectiveness of the bank's internal financial controls and risk management system, and monitoring the effectiveness of the internal audit function. The BAC also ensures the independence of the external audit function by appointing and assessing the performance of the external auditor. It is also responsible for ensuring compliance with laws and regulations affecting financial reporting.

The BRMC is responsible for oversight of the bank's risk management systems, practices, and procedures to ensure their effectiveness in risk identification and management as well as to ensure compliance with the bank's internal policies and the guidelines laid out by the regulator.

The ALCO establishes guidelines on the bank's tolerance for risk and expectation from investment, sets and monitors specific financial targets and Key Performance Indicators (KPIs), monitors the bank's capital, and ensures that management implements the assets and liability policy of the bank.

The BCC's duties include reviewing the bank's credit portfolio KPIs that include concentrations and provisions, ensuring alignment with the bank's credit strategy and risk appetite, and approving credit terms.

These committees complement each other. The BAC provides the critical independent quality assurance, the BCC manages credit risk, and the ALCO committee manages market risk, the Operational Risk Committee manages operational risk, complianceand legal risk, regulatory risk, and reputational risk. In addition to this, the ICT Committee manages IT risks facing the bank and the BRMC oversees all the risks managed by all other Board subcommittees as well as external or emerging risks.

The internal audit function is independent of all other business units and provides assurance of the adequacy and effectiveness of the bank's risk management, control and governance processes. It is headed by the General Manager Internal Audit, who reports administratively to the Managing Director and functionally to the Board Audit Committee. To improve the independence of the internal audit function, its head has unfettered access to the Chairman of Audit Committee and the Chairman of the Board.

The risk management function is charged with providing guidance to the business units and independently reporting and monitoring the risk management systems. The General Manager, Risk and Compliance Division, in conjunction with the Managing Director, is responsible for setting a framework that ensures effective risk management, compliance and control for all risk types across the bank.

The business units take ownership of the risks with the heads of the business units responsible for identification and management of risk in their business units. This is undertaken through regular Risk and Control Self-Assessment exercises.

- **Strategies:** The Board and senior management should identify the bank's long-term goals before it can identify potential events affecting their achievement. The ERM framework ensures that senior management has in place a process to set objectives and that the chosen objectives support and align with the bank's mission and are consistent with its risk appetite.
- **Event identification:** Internal and external events affecting achievement of a bank's objectives must be identified, distinguishing between risks and opportunities. Opportunities are channeled back to management's strategy or objective-setting processes.
- **Risk assessment:** Risks are analyzed by considering likelihood and impact as a basis for determining how they should be managed. Risks are assessed on an inherent and a residual basis.
- **Risk response:** The senior management selects risk responses—avoiding, accepting, reducing, or sharing risk—and develops a set of actions to align risks with the bank's risk tolerances and risk appetite.
- **Control activities:** Policies and procedures are established and implemented to ensure that the risk responses are effectively carried out.
- **Information and communication:** The relevant risk information should be identified, captured, and communicated in a form and timeframe that enables people to carry out their responsibilities.
- **Risk monitoring:** The entirety of ERM is continuously monitored and modifications made as necessary. Monitoring is accomplished through ongoing management activities, separate evaluations, or both.

3.2.2.2 The Risk Appetite

Setting the bank's risk appetite is a core component of a bank's ERM framework. Risk appetite defines the level of enterprise-wide risk that the bank is willing to accept or the capacity to absorb; it should include thresholds for specific actions, such as acquisitions, new product development, or market expansion. While senior management can propose risk appetite levels, the Board must review and adopt the risk appetite or challenge it for further assessment. The evaluation should be based on the risk appetite alignment

Case Study 10: Risk management framework

In one of the banks interviewed, the Board has facilitated the operationalization of the bank's Risk Management Framework as follows. Different Board committees such as the Board Risk Management Committee (BRMC), Board Audit Committee, and the Board Credit Committee in co-operation with Management Committees provide the written principles for overall risk management policies. They also provide the guidelines for the bank's risk identification, measurement, monitoring, and reporting. The execution of the framework is a function of the bank's Enterprise Risk Management Group, which identifies, evaluates, and hedges financial risks with assistance from the bank's strategic business units. The bank has also appointed a Chief Risk Officer (CRO) who has a direct reporting line to BRMC and a dotted line to the CEO. The establishment of a formal risk management framework has helped the bank to ensure that the risks inherent in the bank's products, processes, activities, and new markets are identified early and the risks profiles are regularly reviewed. The bank's risk management process considers various risks, including credit, operations, liquidity, legal, compliance, and strategic risks.

The identification, assessment, prioritization and mitigation of identified risks are completed through periodic Risk and Control Self-Assessment (RCSA) and development of Key Risk Indicators (KRIs) to identify and monitor the risks. Workshops are held with all stakeholders such as the process owners, the Internal Control Department, Internal Audit, and senior management (through the Risk Management Committee) to assess the identified risks, proffer mitigations and then use heat maps based on frequency and impact to prioritize these. This process is further supported through:

- Use of approved processes and templates for documenting identified risks;
- Existence of a strategic framework for the assessment of risks associated with new ventures (markets and products);
- Periodic review of existing products;
- Existence of defined KRIs; and
- Periodic RCSA exercises.

The RCSA process is coordinated by the Operational Risk Management Department, which reports directly to the CRO and the Executive Risk Management Committee. The results of these exercises are also reported to the Board, through the BRMC, on a quarterly basis.

with the bank's solvency requirements, business strategy and stakeholders' expectations. The Board should define, approve and incorporate it in the bank's strategic and tactical plans. An effective risk appetite statement should:[37]

- Include key background information and assumptions that informed the bank's strategic and business plans at the time they were approved;
- Be linked to the bank's short- and long-term strategic, capital and financial plans, as well as compensation programs;
- Establish the amount of risk the bank is prepared to accept in pursuit of its strategic objectives and business plan, taking into account the interests of its customers (e.g., depositors, policyholders) and the fiduciary duty to shareholders, as well as capital and other regulatory requirements;
- Determine for each material risk and overall the maximum level of risk that the bank is willing to operate within, based on its overall risk appetite, risk capacity, and risk profile;
- Include quantitative measures that can be translated into risk limits applicable to business units and at group level, which in turn can be aggregated and disaggregated to enable measurement of the risk profile against risk appetite and risk capacity;
- Include qualitative statements that articulate clearly the motivations for taking on or avoiding certain types of risk, including for reputational and other conduct risks across retail and corporate markets, and establish some form of boundaries or indicators (e.g., non-quantitative measures) to enable monitoring of these risks;
- Ensure that the strategy and risk limits of each business unit align with the enterprise-wide risk appetite statement as appropriate; and
- Be forward looking and, where applicable, subject to scenario and stress testing to ensure that the financial institution understands what events might push the bank outside its risk appetite and/or risk capacity.

Where possible, the risk appetite should be quantified either as a monetary figure or as a percentage of revenue, capital, or other financial measure (such as loan losses). However, less quantifiable risk areas, such as reputational risk, also need to be considered when setting risk appetite levels.

Figure 5 (page 38) is an illustration demonstrating the key steps in developing a Risk Appetite Statement:[38]

The following points on the Risk Appetite Framework (RAF), Risk Appetite Statement (RAS), and risk limits are important to note:[39]

- The RAF incorporates a RAS that is forward-looking as well as information on the types of risks that the bank is willing or not willing to undertake and under what circumstances. It contains an outline of the risk management roles and responsibilities of the people involved , the risk limits established to ensure that the framework is adhered to, and the escalation process where breaches occur;
- The RAS is linked to the bank's strategic, capital, and financial plans and includes both qualitative and quantitative measures that can be aggregated and disaggregated such as measures of loss or negative events (e.g., earnings, capital, liquidity) that the Board and senior management are willing to accept in normal and stressed scenarios; and
- Risk limits are linked to the firm's RAS and allocated by risk types, business units, business lines or product level. Risk limits are used by senior management to control the risk profile and are linked to compensation programs and assessment.
- The RAS should also have the following various components:[40]
  - » **The risk/return trade-off:** The Board needs to show clearly the relationship between the risk that they take and the perceived return. For higher rates of return, the amounts of risks to be taken would be larger; however, this increases the possibility of the bank's losing the resources committed to such products;

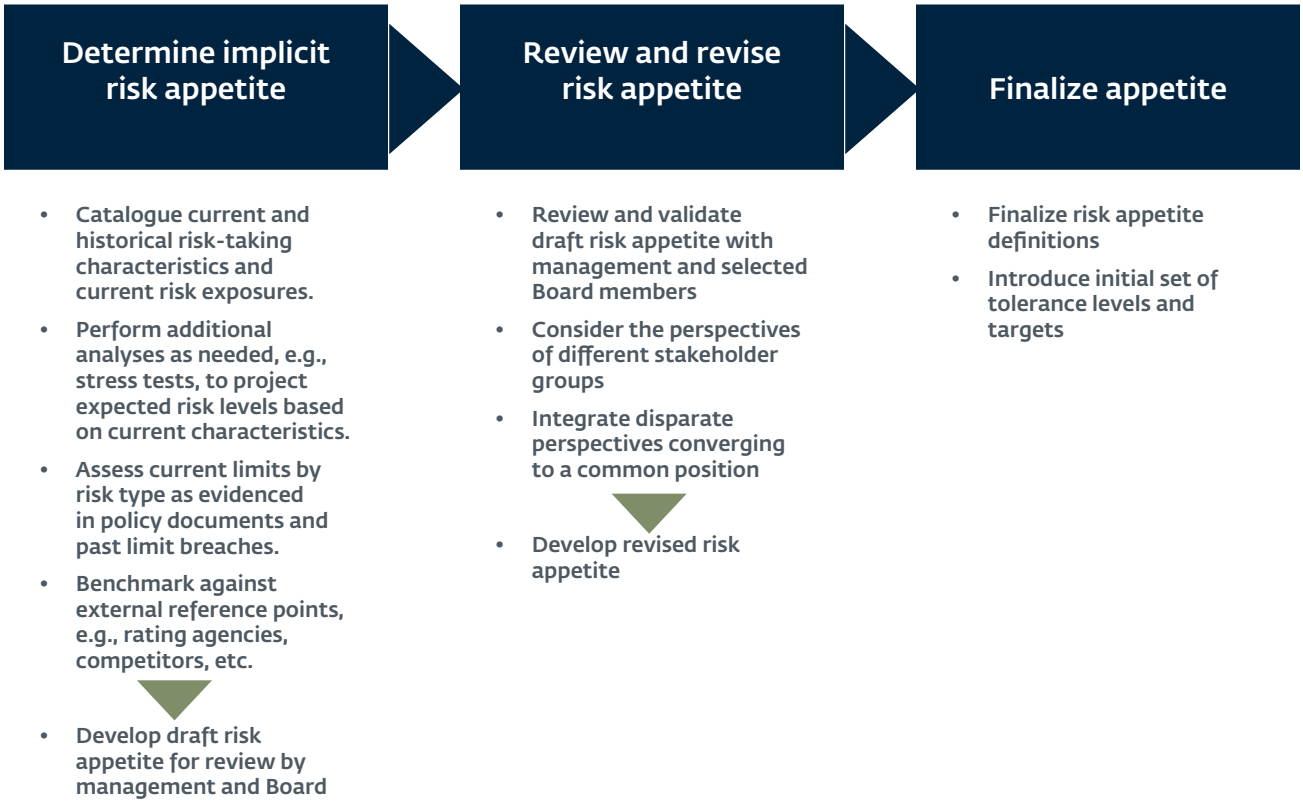
37 Financial Stability Board, *Principles for an effective Risk Appetite Framework*, 2013, pp. 5 – 6.

38 Excerpted from the Report of the NACD Blue Ribbon Commission on Risk Governance: *Balancing Risk And Reward, Appendix C: Developing a Risk Appetite Statement,* published by National Association of Corporate Directors, 2009.

39 Financial Stability Board, *Thematic Review on Risk Governance: Peer Review Report*, 2013, p. 32.

40 International Finance Corporation, *Standards on risk governance in financial institutions,* 2012, p. 8.

Figure 5: Risk appetite statement



» **The interests of various stakeholders:** The bank has various stakeholders, who include the depositors, regulatory authorities, and other lenders. The Board should ensure that the interests of each are considered and agree on prioritization of such interests;

» **Risk identification and measurement capabilities:** The Board should ensure that there is a well-laid-out risk assessment process that identifies the various types of risk and the level associated with the various business strategies. It is desirable to have the risks quantified, but if this is not possible, clear and complete qualitative descriptions should be obtained;

» **Translating risk tolerance into metrics and guidelines:** The Board should aim to ensure that the risk appetite is expressed in standard terms that everyone in the bank can understand and that each business unit has apportioned its risk appetite clearly. This ensures that the risk taking departments are well aware of the acceptable risks they can take and the sanctions one faces should they take any unacceptable risks.

Please refer to Annex 5 for an illustrative Risk Appetite Statement for a financial services organization.[41]

It is important to have an approved RAS, because it:

- Clarifies senior management's authority and boundaries for risk taking;
- Serves as a guide in strategy setting and in allocating resources, where it represents the acceptable balance of growth, risk and return;
- Helps in prioritizing or triggering mitigation actions for risks approaching or exceeding the risk appetite;
- Supports Board oversight and senior management actions to bring/keep the bank's risk profile within its risk appetite or determine whether its risk appetite requires recalibration; and
- Helps make forward-looking and well-informed strategic decisions that can shape the bank's ability to remain

41 Excerpted from the Report of the NACD Blue Ribbon Commission on Risk Governance: *Balancing Risk And Reward, Appendix C: Developing a Risk Appetite Statement*, published by National Association of Corporate Directors, 2009.

profitable while also managing risk prudently in the face of economic, market, and regulatory events.

3.2.2.3 Internal Capital Adequacy Assessment Process

The Internal Capital Adequacy Assessment Process (ICAAP) is a set of sound, effective and complete strategies and processes that allow a bank to assess and maintain – on an ongoing basis – the levels, types, and distribution of its own funds that it considers adequate to cover the risks faced by the bank.

The risk appetite is a key component of a bank's ICAAP, where the objective is to ensure that there is a link between risk and capital adequacy. ICAAP informs the Board of the ongoing assessment of the bank's risks, how the bank intends to mitigate those risks, and the capital levels required, having considered all the mitigating factors. ICAAP is also an important focus of the regulators and may be used to review and assess the capital adequacy and quality of risk management framework of a bank.

ICAAP should have two major components that include an internal process to identify, measure, manage, and report risks that the bank is exposed to or could be exposed to in the future; and an internal process to plan and manage its internal funds so as to ensure sufficient capital adequacy. It should be reviewed by an objective and independent function such as the internal audit function or external consultants at least annually.

Within the bank's risk management framework, ICAAP ensures that the Board and senior management:

- Adequately identify, measure, aggregate, and monitor the institution's risks;
- Ensure that the bank holds adequate internal capital in relation to its risk profile;
- Uses and continually improves the bank's risk management systems; and
- Holds adequate capital commensurate with its current, forecast and stressed risk profile.

The ICAAP process should be in line with the bank's strategic objectives and meet the following requirements:

- Consider all material risks;
- Incorporate prospective assessments;
- Use appropriate methodologies to measure and relate to capital;
- Be adequately formalized and documented;
- Specify the roles and responsibilities assigned to bank functions and business units;
- Be supported by a sufficient number of qualified personnel with the authority necessary to enforce compliance with plans; and
- Be an integral part of management activity.`reasonably be expected to interfere with the independent exercise of his/her best judgment for the exclusive interest of the company.

The Board should establish and approve the general structure of the process, and ensure its prompt adaptation to significant changes in the strategic objectives, and business plans by making full use of results of ICAAP for strategic and decision-making purposes.

ICAAP would enable the bank to,

- Use "what if" analyses to assess its risk exposures under adverse conditions and determine whether the amount of internal capital needed to cover such exposure is in place, or any other actions needed to be taken to reduce the risk; and
- Verify the results and accuracy of the bank's risk assessment models.

3.2.3 QUALIFICATIONS AND EXPERIENCE

Checkpoint:

- ✓ Board qualifications
- ✓ CRO qualifications
- ✓ CAE qualifications
- ✓ Risk and audit staff skills and experience

Those responsible for risk management should have the appropriate qualifications, experience and skills in risk management, bank operations, legal and financial background as appropriate. A carefully crafted plan, which starts from recruitment and continues even after hiring, with the right induction and training plans enhances the Board's qualification and experience. To ensure that the bank has the right mix of skills and experience, the bank should:

- Recruit Board members from a large pool of people to ensure that the Board will be composed of members who possess relevant expertise and will exercise objective judgment. The Board should ensure that at least one of its members has a strong background in risk management and/or internal audit. In addition to banking experience,

selection of independent Board members should further enhance the Board's performance. In addition to this, it may be of great benefit to the bank if one of the members of the Board Risk Committee is a "risk expert"[42] and has any of the following qualifications:[43]

- » Experience as a CRO, CEO, chief finance officer (CFO), or chief compliance officer (CCO) who has successfully owned or managed a risk management program at a bank of comparable size, scope, operations, and complexity;
- » Experience successfully managing significant risks and a range of risks (for instance, beyond a single risk, such as credit or market risk) at a similar bank; and
- » Organizational and leadership skills required to work with committee members, the Board, and management to further the cause of sound risk management in the enterprise.

> A director is identified as "independent" if the Board of Directors will determine that such director meets the requirements established by the Board and is otherwise free of material relations with a company's management, controllers, or others that might reasonably be expected to interfere with the independent exercise of his/her best judgment for the exclusive interest of the company.
>
> —International Finance Corporation, 'Practical Guide to Corporate Governance,' 2009, p. 227

- To ensure that the Board gets the right caliber of the "risk expert" as defined above, the Board should consider the following questions in regard to a risk expert:[44]
  - » Has this person served as a CEO, CRO, CFO, or CCO, or in another position with substantial risk-related responsibilities? How recent is his or her experience?
  - » What was the industry, size, and scope of the organization(s), and which risks did he or she manage or oversee? How do the businesses and risks that the individual previously oversaw compare with those of the company?
  - » What was the nature of regulatory requirements and expectations for risk management in the individual's prior organization?
  - » How hands-on and in-depth is his or her experience? In other words, did he or she just sign off on risk management or oversight reports, or was he or she truly involved?
  - » What was the size of the risk organization and what role did the individual play in developing and overseeing the risk organization?
  - » What were the results of risk management and governance activities during and after this person's watch? What were his or her successes and failures, and how does he or she view them?
  - » How risk averse or risk tolerant is this person in organizational settings?
  - » Has this individual had the experience of identifying, analyzing, monitoring, and reporting on risk to a Board of Directors?
  - » Is this individual a good fit with the Board, executive team, and major shareholders in terms of personality, team orientation, communication skills, and leadership style?
- Have a director's orientation program whose objective is to familiarize new Board members with the bank's risk management process and the Board's roles and responsibilities.
- Ensure that the CRO, CCO, CAE and the members of risk management, compliance, and internal audit functions have relevant professional qualifications and experience, appropriate for the position in line with country-specific education systems and requirements. However, at a minimum, the CRO, CCO, and CAE and employees in the risk management, compliance, and internal audit functions should have extensive experience working in or with banks, particularly in business units such as operations, finance and/or legal departments.

42 "This risk expert role is somewhat analogous to the role of the financial expert required to be on the audit committee by the Sarbanes-Oxley Act of 2002" – Deloitte, *Risk Committee Resource Guide for Boards*, 2012, p. 9.

43 Deloitte, *Risk Committee Resource Guide for Boards,* 2012, p. 9.

44 Ibid.

3.2.4 TRAINING AND CAPACITY BUILDING PROGRAMS

Checkpoint:

- ✓ Board training
- ✓ Employee training
- ✓ Training evaluation

Training is an investment in intellectual capital which generally results in enhanced employee knowledge and skills. It facilitates understanding of complex products and/or service offerings, thereby helping the bank to manage its risks. It involves the imparting of risk management skills and knowledge, concepts, and rules that aim to change the attitude and behavior of the bank employees toward risk.

As risks in the economic, competitive, regulatory, legal, and technological environments are dynamic, risk governance must evolve in response. The bank's leaders must therefore undergo continuous training that may include conferences, selected readings, customized briefings, and courses designed for Board members and senior management in order to:[45]

- Stay abreast of leading practices as risks evolve and as the senior management updates its risk management methods;
- Understand new risks associated with new products and how changes in regulations may increase or decrease risk;
- Periodically benchmark risk governance practices of the bank with its peers, competitors, customers, and suppliers in order to understand evolving practices and evolving expectations of its stakeholders;
- Keep up to date on risk disclosure requirements in communication with external stakeholders; and
- Offer orientation programs for new risk committee members and a module in Board members' orientations to inform them about the risk committee.

The bank should consider if the following questions are answered adequately, with regard to its training program:

- Does the Board receive any training to understand and execute its responsibilities for risk oversight? How often is training conducted and updated?
- Are risk management procedures and protocols documented and communicated? Are there training programs focused on developing a risk awareness culture? How often are these conducted and updated? What is the participation quotient of employees in these?
- Are there perceived weaknesses in the current training programs? In which areas?
- What unexpected risks have impacted the bank recently, and why? What is the training strategy to organize and prepare for such events?

At a minimum, training programs should include the following:

- There should be annual training on creating awareness on risk management to all employees of the bank. The CEO should champion this.
- The training should cover the concepts of risk management, which include definition of risk, risk management, emerging risks, risk assessment / measurement, risk mitigation, and reporting processes, and the roles and responsibilities of the Board members, senior management, and all employees.
- There should be regular monitoring and reporting on the training performed.
- There should be a mandatory induction program / sessions on risk management for all new employees and for new Board members.

See Annexes 6 and 7 for sample training programs for the Board and risk champions, respectively.

45 Ibid., p. 16.

Case Study 11: Risk management training

One bank that was interviewed uses an e-learning platform to disseminate required learnings to the Bank's employees. Courses on financial analysis, financial accounting, credit analysis, securities in banking and internal controls are included on this platform.

Classes are also conducted through a mix of internal and external consultants and courses are a mix of mandatory and optional courses.

For specialized trainings, some employees are selected for initial training so that they can transfer the knowledge acquired to other employees in their departments.

The above training and capacity building programs provide knowledge to employees, giving them a comprehensive vision of risk management within the organization's different sectors, from the theoretical aspects to implementation as a management tool.

3.2.5 BOARD EVALUATION

Checkpoint:

- ✓ Regular assessment of the Board's performance through internal & external reviewers; and
- ✓ Disclosure of risks facing the bank

Board evaluation is a process by which the bank gauges how well its Board is achieving the targets set. The main objective of the evaluation exercise is to improve the effectiveness of the Board's activities.

The following practices ensure that a bank's Board evaluation meets its risk management objectives:

- There should be regular assessment of the Board's performance on risk management oversight, Board composition, experiences, knowledge and skills which should inform better ways as to how the Board should effectively deliver on its mandate.
- The areas of evaluation of the Board Risk Committee, in particular, should include:[46]
  - » The breadth and depth of the Board Risk Committee's knowledge of risk and risk governance and management (including ongoing education);
  - » The independence of the risk committee members from management;
  - » The performance of the chair of the committee and his or her relations with management and the CRO and with the committee;
  - » The clarity of communications with management about risk, and the degree to which these communications have been understood and acted upon;
  - » The quality of Board, risk committee, and management responses to potential or actual financial, operational, regulatory, or other risk events; and
  - » The effectiveness of the information received and reporting about risk by management.

The above is further illustrated in annex 8, in which an illustrative Board risk committee evaluation questionnaire has been included.

- During performance evaluation, the Board should consider the following process:[47]
  - » Select a coordinator and establish a timeline for the evaluation process;
  - » In addition to risk committee members completing the form as a self-evaluation, ask individuals who interact with the risk committee members to provide feedback;
  - » Ask each risk committee member to complete an evaluation by selecting the appropriate rating that most closely reflects the risk committee's performance related to each practice; and
  - » Consolidate the results of such inquiry and evaluation into a summarized document for discussion and review by the committee.
- In addition to self-assessment, commissioning an independent external review of a bank's risk governance policies, procedures, and performance can yield useful benchmarking information and shed light on leading risk governance practices.
- The Board should assess the adequacy of the disclosure of the risks facing the bank in a clearly documented disclosure policy. A disclosure of material circumstances, an annual report, or other disclosures should document the risks affecting the bank's performance and meet the minimum requirements set out by regulatory bodies.
- The bank should have an integrated and detailed program for incorporating feedback from the performance review initiatives and show improvement on implementation of such recommendations.

3.3 RISK GOVERNANCE MATURITY RATING SCALE

Table 4 lists criteria that can be used to assess a bank's maturity against each one of the risk governance best practices. The following key risk governance indicators can be used by banks to undertake a self-assessment and benchmark their risk governance structures against the recommended best practices.

3.4 CONCLUSION

The financial crisis spurred fundamental changes in risk governance practices at banks. In its report,[48] the FSB noted that surveyed financial institutions were ahead of regulatory

46 Ibid.

47 Ibid., pp. 26-29.

48 Financial Stability Board, *Thematic Review on Risk Governance, Peer Review Report*, 2013, p. 17.

Table 4: Criteria that can be used to assess a bank's maturity against each one of the risk governance best practices

Component	Below Standard	Standard	Above Standard
Risk Governance Structure	Lack of a defined governance structure to oversee enterprise-wide risk management. Roles and responsibilities of the Board, CRO and senior management are not defined. A risk appetite statement is not established. The risk management functions are not in existence or do not have adequate resources and support to play their role in risk governance as a second line of defense. The bank does not have an internal audit function, and even where there is one, it lacks independence and/or adequate resources to play its role in providing assurance on risk governance as a third line of defense. Individuals or groups tasked with responsibilities for risk governance lack the appropriate independence.	The Board has documented and approved governance structures and guidelines and its committees have charters that explicitly include their risk management roles and responsibilities. These guidelines have not been communicated throughout the bank. Risk appetite is mentioned in connection with critical topics such as strategy discussions. There is an internal audit function and/or a risk management function, but their recommendations are not positively received and implemented. The individuals or groups tasked with responsibilities for risk governance report to the CEO or equivalent but have no reporting line to the Risk Management Committee or Board.	The Board-approved risk governance structures and guidelines are well understood throughout the bank, and risk management initiatives are continually sustained and strengthened by all key stakeholders who include the Board, senior management, and employees. A Board-approved risk appetite statement is leveraged across the bank to inform all business decisions and supports the enterprise-wide risk management practices. The risk management function is integrated as part of the second line of defense in the risk governance structure. The internal audit function is integrated into the risk governance framework as a third line of defense. The individuals or groups tasked with responsibilities for risk governance have appropriate independence and report directly to the Risk Management Committee or Board.
Risk Management Framework	Lack of a defined risk management framework that defines the bank's risk management processes, functions such as risk identification, assessment, measurement, control design and reporting. Due to lack of a risk framework, the bank's risk appetite levels are not clearly defined. Lack of a clearly defined taxonomy for the explicit and implicit risks covered by the bank's risk management program. Lack of tools and/or methodologies needed to adequately quantify risk(s).	Though the bank has a risk management framework which identifies risk management processes such as risk identification, measurement, and control design and reporting, these practices have not been embedded in the risk culture of the bank and are not followed consistently in the day-to-day activities. Each business unit has its own taxonomy of the risks it faces. There is lack of a unified bank risk profile. Different risk management toolkits are used by the bank in managing the different risks, or each business unit has its own toolkit.	A risk management framework is understood across the bank and leveraged upon by all the risk management stakeholders' to drive the risk management programs in the bank. The bank has a unified classification of risks, and those charged with risk oversight have a unified view of the risks facing the bank. A single risk management toolkit is used, and is accessible to all those charged with risk oversight in the bank to aid in the quantification of risks.
Qualifications & Experience	The Board, CRO, internal audit functions and other persons charged with the responsibility for risk governance do not have the requisite skills and experience.	Some members of the Board have good backgrounds in finance, banking, and audit or risk management. Employees in the Risk Management function and the Internal Audit function have good formal education, credentials and training but skills gaps exist.	A significant number of Board members have a strong finance, audit, and/or risk background. The majority of the Board members and the CRO and his team have excellent formal education and significant industry experience. The Internal audit team has the requisite skills to enable them to play the risk governance role as a third line of defense.
Training and Capacity Building	The Board and pertinent individuals do not receive training to understand and execute their required responsibilities for risk management.	The Board and risk management function receive occasional training to understand and execute their required roles and responsibilities for effective risk management.	The Board and all functions receive regular and focused training to understand and execute their risk management responsibilities.
Board Evaluation	Risk management is not included in performance management systems. There are minimal improvement initiatives resulting from risk management and/or internal audit activities, such as internal reviews, internal or external assessments, user feedback, complaints, and other issues.	Risk management is included in performance management systems for management and not at lower levels There is a high-level program for improvement resulting from activities such as internal reviews, internal or external assessments, user feedback, complaints, and other issues, but this is only deployed superficially	Risk management is integrated with performance management systems and continually adapted based on feedback and changing bank needs. There is an integrated and detailed program for improvement resulting from activities such as internal reviews, internal or external assessments, user feedback, complaints, and other issues.

Adapted from the Global Financial Service Industry (GFSI) Risk Transformation Toolkit, Deloitte Development LLP, May 2013.

and supervisory guidance. In general, surveyed institutions that were most affected by the crisis have made the greatest advancements, perhaps necessitated by a need to regain market confidence. Firms that were less troubled from the crisis, however, have increased the intensity of the measures that they had in place pre-crisis. Some of the most obvious changes include:

- Consolidating and raising the profile of the risk management function across banking groups through the establishment of a group CRO, increasing the stature and authority of the CRO, and increasing the CRO's involvement in relevant internal committees;
- Changing the reporting lines of the risk management function so that the CRO now reports directly to the CEO while also having a direct link to the risk committee;
- Intensifying the oversight of risk issues at the Board through creation of a stand-alone risk committee, supported by greater links with the risk management function and other risk-related Board committees, particularly audit and compensation committees. Cross-membership of the audit committee and risk committee is now quite common, with some firms involving (or at least inviting) the chairman of the Board, even the full Board, onto the risk committee. The time commitment of independent directors has increased considerably over the past several years;
- Upgrading the skills requirements of independent directors on the risk committee and expecting these members to commit more time to these endeavors. The composition of boards has changed considerably, with many non-executive directors now having financial industry experience; the dominance of members from industrial companies or major shareholders is much less than a decade ago;
- Changing the attitude toward the ownership of risk across the firm, with the business line now being much more accountable for the risks created by their activities than previously; and
- In addition to changing the composition and improving the strength of the Board, there have been major developments in how banks analyze risks and the associated tools utilized such as RAFs, stress tests and reverse stress testing. One of the key lessons from the crisis was that reputational risk was severely underestimated; hence, there is more focus on business conduct and the suitability of products, e.g., the type of products sold and who they are sold to. As the crisis showed, consumer products such as residential mortgage loans could become a source of financial instability.

By implementing the recommended practices in this handbook, a bank can attain effective risk governance where:

- Its Board and senior management incorporate a broad outlook on industry risks and integrate risk-aware thinking into strategic decision-making.
- The Board executes its fiduciary responsibilities to ensure that appropriate risk management controls and procedures are in place.
- Capable processes, systems and trained people exist to act on industry intelligence in a timely and coordinated manner.
- A consistent and holistic approach is used across the bank in managing different classes of risk in an effective and efficient manner.

In addition to the Board's risk governance responsibility, it is charged with oversight of the bank's incentives and compensation programs. Incentives play a particularly important role, as they help shape the employees' attitudes toward assuming risk. Incentive programs in banks and recommended best practices are discussed in the next chapter.

4 Incentive Programs in Banks

"The dictionary tells us incentives are things that incite an action. Firms need to ask what type of action they want to incite. Is it to get the best deal for the customer, or the person or the firm selling the product?"

—Martin Wheatley, Former Managing Director of the Financial Services Authority (FSA), United Kingdom (UK)

4.1 INTRODUCTION

Incentive programs linked to risk performance grew out of companies' desires to reduce fixed compensation costs and focus on pay for performance. They were considered "pay at risk" because, unlike guaranteed compensation such as salary and benefits, incentive payouts depended on the achievement of tangible, predefined performance goals. Banks generally considered such incentive pay as a positive means of aligning pay and performance, encouraging senior management to make the right decisions, and driving the right results. However, this is thought to have lured some members of senior management to take significant financial risks to accrue significant rewards.[49]

In a Deloitte Banking Industry Survey[50] released in May 2013, bankers indicated that the main causes of the banking industry's cultural problems were misaligned incentives and poor leadership. Employee incentive programs reinforced failures at the top.

Better risk management and alignment of pay with meaningful, long-term performance address shortcomings in incentive programs seen as a contributor to the global financial crises. Banks should scrutinize their incentive programs to see how they factor in their business strategy, risk profile, and potential business risks. Incentive programs now advocate for and encourage ownership of risks by business units and specific employees.[51]

At a Glance

Recommended best practices in Incentive Program

- Board level responsiblity for the program
- Formal incentive program
- Aligning incentives to the bank's risk horizon
- Transparent incentive reporting
- Creating awareness

49 S. O'Donnell, "Executive incentive practices: Post-TARP," *Bank Accounting & Finance*, 2009, p. 18.

50 Deloitte, *Culture in banking: Under the microscope,* 2013, p. 2.

51 S. O'Donnell, "Executive incentive practices: Post-TARP," *Bank Accounting & Finance*, 2009, p. 19.

4.2 BEST PRACTICES IN BALANCED INCENTIVE PROGRAMS AT BANKS

Checkpoint:

- ✓ Board oversight on development and operation of program
- ✓ Balance of risk and financial results
- ✓ Involvement of the risk management function in the design of the program
- ✓ Shareholders' approval of the incentive program

Due to the role imbalanced incentive programs are perceived to have played in the global financial crisis which started in the summer of 2007, various bodies such as the FSB and the Basel Committee for Banking Supervision have published guidance for improving the linkages between effective risk management programs in banks and compensation. Other parties like the World Bank, IMF, IIF, UK FSA (which has since been split into PRA and FCA), regulatory authorities, and professional services organizations have published papers and guidance materials to improve bank incentive programs so that they more closely link long-term performance to compensation incentives. Below is a summary of key recommendations from some of these guidelines as well as market best practices which a bank can follow in implementing or assessing its incentive program:

- **Board-level responsibility for the incentive compensation programs:** The Board has the overall responsibility for the design and operation of the bank's incentive compensation programs. They may consider greater input and scrutiny from shareholders' perspective, including approval of some aspects.
- **Establishment of a formal risk-based incentive compensation program:** The bank should establish incentive programs that are formal and documented. The compensation programs should be a mix of variable and non-variable aligned to performance measures which encourage sound risk- taking.
- **Aligning incentive payout to the bank's risk horizon:** Incentive compensation payout schedules must be sensitive to the time horizon of risks.
- **Performance measurement based on level of risk decision:** Risk metrics should be included in the Board and senior management's KPIs. These targets should then be cascaded to all employees.
- **Transparent reporting on incentive payout:** The bank should disclose how the Board of Directors, senior management, and employees are paid, and the relationship between the payments and the bank's performance.
- **Creating awareness in the bank on the risk-based incentive program:** The bank should create awareness of its incentive compensation programs to accelerate buy-in and support from all employees.

4.2.1 BOARD LEVEL RESPONSIBILITY

The Board has the ultimate responsibility of ensuring that the bank's incentive program for all employees and senior management is appropriately balanced and does not jeopardize the bank's safety and soundness. The bank's incentive program should be aligned to its strategy, goals, and performance. A Board that analyzes incentive compensation and the potential impact on risks should actively oversee the development and operation of a formal incentive program, incentive policies, systems, and the related control processes through an established remuneration/compensation committee.

As part of its corporate governance responsibility, the Board should consider the relationship between incentive compensation and risk, especially for the Board and senior management. To carry out this role effectively, Board members of the compensation committee should have a comprehensive understanding of the bank's risk profile and possess some level of expertise and experience in risk management and compensation practices in the financial services sector that is appropriate for the nature, scope, and complexity of the bank's activities. They should ensure that the design of the incentive compensation programs balance risk and financial results in a manner that prevents employees from exposing the bank to imprudent risks. Multiple levels of performance should be incorporated, such as overall bank performance, business unit, and individual performance, and also should ensure that the bank's risk management function is involved in the design and review of the incentive compensation program.

The above was further stressed in a recent position paper on remuneration by the European Confederation of Directors' Associations (ecoDa), stating, "It is important to stress that evaluating executive directors' performance and fixing their remuneration is one of the Board's main duties".[52] As part of the Board's duties, it should focus on ensuring transparency in director and senior management remuneration. Incentive programs for other bank employees should borrow on the

52 European Confederation of Directors' Associations, *ecoDa's response to the European Commission's Green Paper on corporate governance in financial institutions and remuneration policies*, 2011, p. 22.

same principles applied to senior management programs as approved by the compensation committee. This can be delegated to an HR management committee as seen appropriate by the Board. Good practice may be best advanced through dialogue between boards, shareholders, and financial regulators on the basis of corporate governance codes—rather than through regulation. Besides their decisive role in the determination of the remuneration of non-executive directors, the bank's shareholders should always have a say in the remuneration policy of executives (through a "say on pay").

The bank's shareholders should approve the incentive compensation program. The total cost of the incentive plans paid out should be an agenda item in the shareholder's meeting and as part of the bank's annual report. The Dodd-Frank Act in the US enacted in 2010 laid out specific requirements on how shareholders' "say on pay" should be managed. In addition to including the CEO's pay for shareholders' approval, the Act makes the following inclusions on other employees of the institution:[53]

- Disclosing the relationship between the compensation costs of the senior management and the company's financial performance; and
- Disclosing the median annual total compensation of all employees (except the CEO), the annual total compensation of the CEO, and the ratio of the median employee total compensation to the CEO's total compensation.

Shareholders should therefore be encouraged to attend the bank's annual and/or extraordinary general meeting so that they can provide input and/or voice their concerns, if any, on the incentive compensation payouts.

However, in systemically important financial institutions, financial regulators could be an additional source of monitoring for the Board and senior management remuneration policy, specifically taking the interests of other stakeholders such as shareholders, customers, or other banks into consideration."[54] While important, regulation with respect to the incentive plans and level of remuneration should not be excessively prescriptive and more "principles based;" otherwise there is a risk of potential unintended distortion of remuneration practices.

The effectiveness of the compensation committee in a bank determines whether the incentive plans established encourage prudent risk taking.

To facilitate a balanced incentive program, the Board should ensure the following are in place:

- **Formal establishment of a compensation or equivalent committee:** The Board should establish a committee on compensation to have an active role in directing and controlling the compensation policies and practices of the bank. The committee's primary responsibility should be setting appropriate and supportable compensation programs aligned to the bank's business mission and strategy and other interests such as talent management. In its duties, the committee should consider the following issues:
  - » The total value of all cash and non-cash benefits provided to the Board and senior management, including, but not limited to, performance-based pay, retirement benefits, and severance pay;
  - » Compensation of the bank's employees with comparable expertise in the banking industry;
  - » The bank's financial condition and risk appetite; and
  - » Any fraudulent act or omission, breach of trust or fiduciary duty, or insider abuse with regard to the bank's operations and market conduct.

  The compensation committee should meet with the senior management, the risk and HR functions, or compensation experts regarding compensation matters, as deemed necessary.
- **Independent and/or non-executive directors as members of the compensation committee:** The bank should aim at ensuring that the compensation committee comprises non-executive directors, the majority of whom should be independent directors to guard against any potential conflicts of interest. A compensation committee determines that the bank's compensation and benefits packages are aligned with prudent risk taking and do not provide excessive benefits or lead to imprudent risk taking in the bank.
- **Regular review of the independence and performance of the compensation committee or its equivalent:** There should be a regular assessment of the independence of committee members. The performance of the compensation committee should also be evaluated against the mandate set for the committee and the achievement of the objectives of the incentive compensation plans.

53 United States Federal Law, *Dodd-Frank Wall Street Reform and Consumer Protection Act,* 2010, Subtitle E — Accountability and Executive Compensation.

54 European Confederation of Directors' Associations, *ecoDa's response to the European Commission's Green Paper on corporate governance in financial institutions and remuneration policies,* 2011, p. 23.

Case Study 12: Board level responsibility for compensation

In an effort to establish a robust and objective remuneration and incentives program, the Board at one of the banks referenced in this study has a Board Nomination and Remuneration Committee composed of three independent non-executive directors. The committee meets bi-annually and is responsible for:

- Evaluating the performance of the individual Board members and the CEO;
- Setting the remuneration policies and strategic objectives of the Board and the CEO;
- Setting policies on employee incentives such as bonuses; and
- Setting the policies for the Employee Share Ownership Plan (ESOP) and providing requisite guidance to the Plan's's Trustees.

- **Establishment of a formal risk-based incentive compensation program:** The Board has a critical role of operationalizing risk-based incentive programs through a formal risk-based incentive program framework. This is discussed in detail in section 4.2.2 below.

4.2.2 ESTABLISH A FORMAL INCENTIVE PROGRAM

Checkpoint:

- ✓ Identification of risks facing the incentive program
- ✓ Involvement of risk function in designing incentive program
- ✓ Regular assessment of the incentive program
- ✓ Proper documentation of the incentive program

There is increased expectation that banks should ensure proper Board oversight, implement enhanced controls and policies, improve documentation, and revise their incentive plans to consider mitigation strategies. To achieve this, the bank should establish incentive programs that are formal, performance based, and documented with pre-defined objective goals.

The bank should have a formal incentive program, which provides for:

Identification of the full spectrum of risks facing the bank's incentive scheme:[55] Banks should have a systematic and documented approach to identify the full range of risks that could compromise the safety and soundness of the institution. As already noted, risks can only be managed effectively if the bank knows where and what they are. It is recommended that the compensation committee, with support from other functions as appropriate, compile a complete list of major risks associated with all of the bank's incentive plans and identify the employees and business units responsible for controlling each risk.

Performance measures:[56] As per the Basel Committee on Banking Supervision: "performance measures play an important role for the variable part of remuneration packages, as the value of remuneration depends on some kind of performance." Ultimately, performance can be defined as the degree to which the employee has achieved his or her objectives. Because of that, performance measures are an essential tool for linking remuneration policies with both the bank's strategy and the broader risk management framework. The Basel committee advocates that "both qualitative and quantitative performance measures should be considered. While performance measures are normally focused on financial metrics, it is also important that financial institutions include non-financial metrics in developing the risk-based remuneration hurdles. Performance measures also play a vital role in risk adjustment as they deliver the input for such a correction, regardless if they are applied ex ante or ex post. In the case of ex post application, performance measures can serve not only as claw-back[57] or malus[58] triggers, but are also embedded in the design of deferred remuneration plans. Incorporating risk considerations in performance measurement can be achieved both by using risk metrics to correct measures

55 L. Hay, *Trends and issues: Directors' accountability for ensuring risk-based compensation programs*, Pearl Meyer & Partners LLC, 2012, p. 1.

56 Basel Committee on Banking Supervision; *Range of Methodologies for Risk and Performance Alignment of Remuneration*, May 2011. p. 17.

57 A clawback provision is a contractual clause that gives the bank an inherent right to reclaim some or all the incentive payouts given to an employee. This clause is usually invoked due to some special circumstances outlined in the contract (for example, material misstatements in the bank's financial statements or a contribution to the damage of the bank's reputation).

58 A malus provision is a contractual clause that gives the bank an inherent right to reduce the incentive payouts that have been vested but not yet paid to an employee. It allows the bank to revise the vested incentive payments if the performances over a multi-year period are below the KPIs when the original incentive was granted.

which are not risk adjusted measures and also by employing metrics which are adjusted for risk in the first place." The clawback clauses operate by requiring the employee to return a specified amount of money to the bank, whereas the malus clauses operate by affecting the vested amounts (reduction of the amount due but not paid).

Risk adjustments:[59] When creating remuneration plans, a financial institution should ensure that incentives to take risk are constrained by incentives to manage risk. The best way to achieve this outcome is to vary incentive-based remuneration according to risks taken (ex ante) and risks realized (ex post). There are two points at which this can be done:

- Ex ante – by adjusting remuneration for risk as it is accrued and awarded, to take into account potential adverse developments in the future. An ex ante is a "discount" on an incentive payout. The discount is designed to reflect the level of risk exposure being taken on by the bank at the time of underwriting but has not yet materialized; or
- Ex post – by adjusting accrued remuneration during (e.g., through a malus clause) or after (e.g., through a clawback clause), a deferral period in the light of experience and observations of risk and performance outcome. Ex post adjustments are designed to incorporate risk outcomes after a reasonable deferral period that allows risks to materialize.

Both methods rely on the bank's having in place reliable processes to measure potential risk exposures and/or risk experience, and which are capable of "arm's length" verification.[60]

A key driver for risk-adjusted remuneration is that it is intended to influence employee and senior management behavior within the bank. For incentive programs to be effective, this process should ideally be supported by strong governance and a culture of prudent risk taking within any organization.[61] The balance between base pay—for example, salaries—and incentive payouts might contribute to reduce the effectiveness of incentive plans when, for instance, the base pay is not sufficient to make the incentive payout genuinely discretionary or when the incentive payout is too small.[62]

Involvement of risk management, compliance, and internal audit function in the design of incentive programs:[63] While there is no "one-size-fits-all," banks should consider for each role/function what type of risk adjustment features are most appropriate. The risk management, compliance, and internal audit functions should be involved in the design and monitoring of incentive compensation programs because of their skill and expertise, and promote sound governance practices in the definition and implementation of the incentive programs.

At banks where risk management, compliance, and internal audit personnel are intensely involved in basic design decisions of the incentive compensation system, as well as in determining details of the risk-related elements of the incentive compensation, adoption of such incentive programs has tended to be faster. At banks where the risk, compliance, and internal audit functions play a peripheral or informal role, progress has tended to be slower, primarily because other personnel tend to have less experience and expertise in designing risk identification and measurement features.[64]

To ensure effective alignment of the programs, the risk management, compliance, and internal audit functions should be involved in the review as well as in the design and monitoring of short- and long-term incentives. Additionally, given their role as "gatekeepers," their own incentive compensation programs should ensure objectivity and not be tied directly to the business units they monitor. As per the Commission of the European Communities' recommendations on remuneration policies in the financial sector, "Employees engaged in control processes should be independent from the business units they oversee, have appropriate authority, and be compensated in accordance with the achievement of the objectives linked to their functions, independent of the performance of the business areas they control."[65] When incentive programs for employees and senior management in these roles are being defined by the remuneration committee, they should take into account the relevance or applicability of risk-adjusted pay matrices to drive the right behavior, given their mandate within the bank.

59 Basel Committee on Banking Supervision; *Range of Methodologies for Risk and Performance Alignment of Remuneration,* May 2011, p. 17.

60 Ibid., p. 18.

61 Ibid., p. 11.

62 Ibid., p. 18.

63 Board of Governors of the Federal Reserve System, *Incentive Compensation Practices: A Report on the Horizontal Review of Practices at Large Banking Organizations,'*2011, p. 21.

64 Ibid., p. 22.

65 Report Issued by the Commission of the European Communities, Brussels, 30.4.2009, C (2009) 3177, *Commission recommendation on remuneration policies in the financial services sector,* p. 8.

Regular evaluation and assessment of the incentive programs: To assess the effectiveness of the incentive programs, banks should regularly review whether the design and implementation of their incentive compensation programs encourage appropriate risk-taking decisions. They should correct deficiencies discovered and make improvements as suggested by the findings. The internal audit function plays a critical role in reviewing compliance with policies and procedures geared toward incentive compensation. An incentive program may be implemented as intended, but it may still fail to achieve the desired relationship between risk and incentive because features of its design and operation do not work out as expected. Detecting such scenarios requires that a bank monitor relationships among measures of short- and long-run financial performance, amounts of incentive compensation awards, measures of risk and risk outcomes, amounts of ultimate payments of deferred incentive compensation, and other factors relevant to incentive compensation decisions.[66] This should ultimately be the responsibility of an established compensation committee.

Proper documentation: All programs, policies, monitoring procedures, and governance protocols should be complete and clearly documented. Banks should seek to document all incentive plans as well as monitor and control procedures. Where discretion is applied, documentation of rationale and methodology should be included. Committee minutes should reflect discussions and considerations of risk relative to plan designs and payouts.[67]

4.2.3 ALIGN INCENTIVE PAYOUTS TO PRUDENT RISK TAKING AND BANKS' RISK HORIZON

Checkpoint:

- ✓ Align incentive to risk
- ✓ Defer incentives
- ✓ Use a mix of cash and shares in incentive payouts

An employee's incentive compensation should take into account the risks that the employee takes on behalf of the bank. Incentive compensation should take into consideration prospective risks and risk outcomes that are already realized. Incentive compensation should be adjusted for all types of risk which the banks have agreed to be part of the incentive program. Two employees who generate the same short-run profit but take different amounts of risk on behalf of their company should not be treated the same by the incentive compensation program. In general, both quantitative measures and human judgment should play a role in determining risk adjustments. Risk adjustments should account for all types of risk, including difficult to-measure risks such as liquidity risk, reputation risk, and cost of capital.[68]

To align incentive payouts to prudent risk taking:

- Incentive compensation payout schedules must be sensitive to the time horizon of risks. Profits and losses of different activities of a bank are realized over different periods. Variable incentive payments should be deferred accordingly. Payments should not be finalized over short periods where risks are realized over long periods. The Board should question payouts for income that cannot be realized or whose likelihood of realization remains uncertain at the time of payout. A bank should introduce forward-looking long-term incentive plans for senior management who occupy key strategic roles, based on performance achievements. Incentive policy should factor in linkage between variable components and performance measures: [69]
  - » Where the remuneration policy includes variable components of remuneration, banks should set limits on the variable component(s). The non-variable component of remuneration should be sufficient to allow the bank to withhold variable components of remuneration when performance criteria are not met;
  - » Award of variable components of remuneration should be subject to predetermined and measurable performance criteria;
  - » Performance criteria should promote the long-term sustainability of the bank and include non-financial criteria that are relevant to the bank's long- term value creation, such as compliance with applicable rules and procedures, standards of conduct and behavior;
  - » Incentives should take into account the right mix of quantitative and qualitative measures that should be assessed for individual employees, based on their roles, to

66 Board of Governors of the Federal Reserve System, *Incentive Compensation Practices: A Report on the Horizontal Review of Practices at Large Banking Organizations,* 2011, p. 23.

67 Office of the Comptroller of Currency, *The role of a national bank director: The director's book,* 2010, p. 24.

68 Financial Stability Forum, *FSF principles for sound compensation practices,* 2009, p. 2.

69 Adapted from Report Issued by the Commission of the European Communities, *Commission Recommendation complementing Recommendations 2004/913/EC and 2005/162/EC as regards the regime for the remuneration of directors of listed companies,* p.5.

Case Study 13: Performance measurement

To encourage the right risk behavior, one bank has established Key Performance Indicators (KPIs) to evaluate and reward the bank's employees for prudent risk decisions. It rewards employees by use of incentives such as bonuses and equity. The bank has a formal process for identifying the risks it faces through its integrated risk management practices. The risk management function is involved in the design of the incentive program by providing and deciding which key risk indicators should be included in determining KPIs for different working staff groups.

The incentive program features quantitative and qualitative performance rating systems. The quantitative performance rating system takes quantitative indicators such as profit and non-performing loan ratios into consideration, while qualitative performance rating system features 360° staff performance rating: an employee's supervisors, peers and staff at junior levels give ratings on an employee's performance.

Those who contravene the bank's policies and rules are subject to the sanctions stipulated in the code of conduct which include warnings, economic punishment such as fines, and administrative punishment.

Deferral of incentive payouts is done on a case-by-case and is based on rules and policies formulated by the Remuneration and Appraisal Committee.

The details of the incentive program are included in the bank's internal policies and rules and are communicated to the employees through the bank's intranet, emails, and print outs.

ensure that the incentives drive the right behavior and not financial metrics such as revenue generation only; and

  - Where a variable component of remuneration is awarded, a major part of the variable component should be deferred for a minimum period of time. The part of the variable component subject to deferment should be determined in relation to the relative weight of the variable component compared to the non-variable component of remuneration.

- Incentive compensation outcomes must be symmetrical with risk outcomes. The incentive plan within a bank should link the size of the bonus pool to its overall performance. Employees' incentive pay-outs should be linked to the contribution of the individual and business to such performance.
- Measuring and evaluating performance or awards should be on a multi-year basis to allow for a greater portion of risks and risk outcomes to be observed within the performance assessment horizon. To be effective, multi-year assessments should give appropriate weight to poor outcomes due to past decisions. Otherwise, adverse outcomes may be effectively ignored due to an emphasis on current-year performance.
- There should be a provision for clawback or recovery on excess compensation paid in the event of scenarios such as material misstatement in financial reporting, ethical or criminal misconduct or other agreed-upon conditions.
- There should be policies that restrict severance agreements (significant benefits in case of termination of employment) and rewards for failure. This should include prohibition on paying severance agreements in the event of non-performance.[70] Severance incentives should consider the following at a minimum and not severance incentives should consider:[71]
  - Contractual arrangements should include provisions that permit the bank to reclaim variable components of remuneration that were awarded on the basis of data which subsequently proved to be manifestly misstated;
  - Termination payments should not exceed a fixed amount or fixed number of years of annual remuneration, which should, in general, not be higher than two years of then on-variable component of remuneration or the equivalent thereof; and
  - Termination payments should not be paid if the termination is due to inadequate performance.
- The mix of cash, shares and other forms of compensation must be consistent with risk alignment. The mix will vary

70 Institute of International Finance & Oliver Wyman, *Compensation Reform in Wholesale Banking 2010: Progress on implementing global standards*, 2010, p. 43.

71 Adapted from Report Issued by the Commission of the European Communities, *Commission Recommendation complementing Recommendations 2004/913/EC and 2005/162/EC as regards the regime for the remuneration of directors of listed companies*, p. 5.

depending on the employee's position and role. The bank should be able to explain the rationale for its mix. Incentive policies should factor in the following good practice guidelines with regard to shares and share options:[72]

- » Shares should not vest for at least three years after their award;
- » Share options or any other right to acquire shares or to be remunerated on the basis of share price movements should not be exercisable for at least three years after their award.
- » Vesting of shares, and the right to exercise share options or any other right to acquire shares or to be remunerated on the basis of share price movements, should be subject to predetermined and measurable performance criteria;
- » After vesting, executive directors should retain a number of shares until the end of their mandate, subject to the need to finance any costs related to acquisition of the shares;
- » The number of shares to be retained should be fixed, for example twice the value of total annual remuneration (the non-variable plus the variable components); and
- » Remuneration of non-executive or supervisory directors should not include share options.

The above is the responsibility of the compensation committee and can be delegated across the various business units as required.

4.2.4 TRANSPARENT INCENTIVE COMPENSATION REPORTING

Checkpoint:

- ✓ Incentive compensation disclosure
- ✓ The relationship between performance and incentive payout

The bank should ensure that disclosures relating to how compensation decisions are made, how performance criteria are established, and how performance results lead to incentive payouts help improve employee incentive reporting clarity. The main purpose of ensuring clarity in compensation reporting throughout the bank is to ensure that compensation issued to employees match their performance and the business performance of the bank within a set duration.

As a best practice, banks should ensure transparency around incentive programs through:

- Clear, comprehensive, and timely information on the bank's incentive programs to facilitate constructive engagement by all stakeholders.[73]
- Information regarding the relationship between the bank's financial performance and the total incentives actually paid.[74]
- Disclosures in an independent remuneration policy statement or disclosures in annual financial statements that can be guided by regulatory requirements (where applicable), the nature, the size, as well as the specific scope of activities of the bank.

The following information can be considered for transparency and disclosure:[75]

- Information concerning the decision-making process used for determining the remuneration policy, including, if applicable, information about the composition and the mandate of a remuneration committee, the name of the external consultant whose services have been used for the determination of the remuneration policy, and the role of the relevant stakeholders;
- Information on linkage between pay and performance;
- Information on the criteria used for performance measurement and the risk adjustment;
- Information on the performance criteria on which the entitlement to shares, options or variable components of remuneration is based; and
- The main parameters and rationale for any annual bonus program and any other non-cash benefits.

4.2.5 CREATING AWARENESS OF THE COMPENSATION PROGRAMS

Checkpoint:

- ✓ Staff emails
- ✓ The intranet
- ✓ Periodic in-house publications
- ✓ During staff training

The importance of the incentive program's communication is frequently underestimated. All staff members should be made aware of the bank's compensation program to help stimulate

72 Ibid.

73 Financial Stability Forum, *FSF principles for sound compensation practices,* 2009, p. 3..

74 Institute of International Finance & Oliver Wyman, *Compensation Reform in Wholesale Banking 2010: Progress on implementing global standards*, 2010, p. 27.

75 Report issued by the Commission of the European Communities, Brussels, 30.4.2009, C (2009) 3177, *Commission recommendation on remuneration policies in the financial services sector,* p. 8.

Case Study 14: Transparency guidelines in India

There has been considerable effort to improve the incentive programs in the financial services industry since the global crises. The Financial Stability Board issued 9 principles of sound compensation practices in 2009 to encourage the right practices across various regions and discourage imprudent risk taking as a result of incentive programs in place.

In 2012, the Reserve Bank of India issued guidelines[a] on the compensation of bank employees to be implemented from the financial year 2012–2013. To encourage transparency in a bank's incentive programs, the annual report should disclose the following information:

- Composition and mandate of the remuneration committee;
- Design and structures of the remuneration processes and key features and objectives of the remuneration policy;
- The risk management processes of risks facing the remuneration policy;
- How the bank links performance management with its levels of remuneration;
- The bank's policy on deferral and vesting of variable remuneration and the criteria for adjusting the deferred remuneration before and after vesting;
- A description of the different forms of variable remuneration that are used and the rationale for using such;
- Number of meetings held by the remuneration committee during the year and payment to its members;
- Number of employees that have received a variable remuneration award during the financial year;
- Number and total amount of sign-on awards made during the financial year;
- Details of guaranteed bonus, if any, paid as joining / sign-on bonus;
- Details of severance pay, in addition to accrued benefits, if any;
- Total amount of outstanding deferred remuneration, split into cash, shares and share-linked instruments and other forms;
- Total amount of deferred remuneration paid out in the financial year;
- Breakdown of amount of remuneration awards for the financial year to show fixed and variable, deferred and non-deferred components;
- Total amount of outstanding deferred remuneration and retained remuneration exposed to ex post explicit and/or implicit adjustments; and
- Total amount of reductions during the financial year due to ex- post explicit adjustments.

a Reserve Bank of India – Guidelines on Compensation of Whole Time Directors/CEOs/Risk takers and Control function staff, etc., 2012 (http://rbidocs.rbi.org.in/rdocs/notification/PDFs/349CC130112.pdf)

effective risk taking. Mechanisms for sharing information about the compensation program can be conducted through the institution's formal communication channels, such as staff emails, intranet, and routine publications, and during regular training programs.

The bank should ensure that staff members understand the incentive programs' mechanics and the reasons for the program. If employees do not accept the program, it will have limited or potentially even counterproductive impact on their motivation and decisions about taking and managing risks.

4.3 BALANCED INCENTIVES PROGRAM MATURITY RATING SCALE

The maturity scale (Table 5) has been provided to help assess an organization's maturity with regard to a balanced incentives plan to aid in effective risk management.

Case Study 15: Creating awareness of the incentive programs

In order to create awareness of their incentive program, some banks ensure that human resource procedure manuals and salary administration policies are regularly updated and available to all the bank's employees through the bank's intranet portal. Supervisors are also trained on these policies and procedures so that they can impart such knowledge to the staff in their departments.

Any feedback obtained through these sessions is channeled to the compensation team that clarifies any doubts and concerns about the incentive programs. This ensures there is a process of continuous communication and improvement on the bank's incentive programs.

Table 5: Maturity scale

Component	Below Standard	Standard	Above Standard
Board level responsibility	The Board is not involved in the design of the bank's incentive program, as this role is played by the Human Resource department. The bank does not have a compensation committee to oversee the compensation process.	The Board is involved in the design of the incentive programs for senior management and heads of business units but no other levels of employees. The bank has a compensation committee responsible for setting appropriate and supportable pay programs aligned with the bank's business mission and strategy and other best interests. However, such committees are not effective enough to meet such obligations, and their decisions are sometimes overridden.	The Board is involved in the design of the incentive programs of all bank employees. The bank has an effective compensation committee mandated with the responsibility for setting appropriate and supportable pay programs that are aligned with the bank's business mission and strategy and other best interests.
Formal incentive program	The bank does not have a formal approved incentive program to reward risk taking. Risk management and internal control personnel are not involved in the design or review of incentive programs as part of a broader strategy to incorporate risk metrics in compensation calculations and a general strengthening of the risk governance functions of these two functions.	The bank has a formal incentive program which is sometimes over-ridden due to other business pressure such as growth requirement versus the risk factors of the opportunity. Risk management and internal controls personnel have minimal involvement in the design and review of the bank's incentive program, and their input does not always factor in the final incentive plans.	There is a formal incentive program which is followed across the Board. Compensation plans are aligned to long-term performance. The bank seeks the advice of its risk management and control design functions in the design and review of the incentive programs.
Align incentive payout to risk horizons of the bank	The bank relies mostly on short-term incentive plans in the compensation of its employees. The growing significance of long-term incentive planning has not been taken into consideration. Risk management is not included in performance management systems.	The bank considers both short-term and long-term measures in its incentive planning. Compensation payments are closely linked to the bank's future performance. Risk management is included in performance management systems for management, but not at lower levels.	The bank has an effective incentives plan with the right clawback policies on incentives compensation. The plan considers both short-term and long-term measures and the effects on the employee. Risk management is included in performance management systems such as "balanced scorecards." Key Performance Indicators for management and lower levels are continually adapted. based on feedback and changing bank needs.
Transparent incentive compensation reporting	There is no clear, transparent communication of compensation programs.	There is communication regarding compensation programs, flowing downward in the bank.	Consistent communication occurs, flowing upward, downward, and across the bank, as well as disclosures with external parties.
Creating awareness on the incentive program	Though there is an incentive program, employees are not fully aware of how it works and the inputs that are considered in determining total compensation.	Some of the employees, especially at the senior levels, understand the incentive compensation programs fairly well.	Employees throughout the bank are aware of how the incentive compensation programs are designed and how they influence their pay.

Adapted from the *Global Financial Service Industry (GFSI) Risk Transformation Toolkit*, Deloitte Development LLP, May 2013.

4.4 CONCLUSION

From the review of the responses provided during the study, most banks in the emerging markets are still in the nascent stages of developing balanced incentive programs. However, some of the regulators require some of the recommended best practices that include formation of a Board committee responsible for compensation in the bank. As there are no stringent disclosure requirements, most banks do not disclose the total compensation for members of their Board or the senior management team.

A bank's risk profile is ultimately the result of the many decisions made each day as employees seek to accomplish the bank's business objectives.

For optimal incentive programs, it is recommended that the bank's Board should:

- Provide oversight in the development and operationalization of the incentive programs;
- Ensure alignment of these programs with the bank's risk horizon,
- Ensure accurate measurement and incorporation of risk metrics in performance assessment;
- Promote transparent reporting; and
- Create awareness of the incentive programs, so as to eliminate ambiguity.

Effective incentive and compensation practices within a bank should be aimed at striking a balance between the bank's practices and the existing banking regulations, fluctuating market conditions, and public perceptions. There should be greater attention paid to the impact of incentives on the risk profile and effective use as a tool to drive the desired behavior and risk culture.

5 Conclusion

Research continues to show that effective risk management goes beyond establishing an Enterprise Risk Management (ERM) Framework as a "check the box" exercise to meet regulators' requirements. The financial crisis which emerged in 2007–2008 indicates that though risk management processes were in place to identify, assess, and manage risk, shortcomings became evident where these processes were not systematically refreshed based on changing conditions.

Beyond having an ERM framework, banks must take into consideration the impact of soft qualitative factors in their operating environment, which influence their risk management programs. Within the emerging markets where many banks may still be in the implementation stage of ERM frameworks, it is important to incorporate lessons learned in the developed markets and to integrate the soft qualitative factors that influence the effectiveness of their risk management programs. Research continues to show that a weak risk culture, poor risk governance, and unbalanced incentive compensation contribute heavily to financial industry failures.

As noted in a recent publication by the Financial Times, financial firms are increasing their risk appetite as they search for better returns. The Board and senior management should therefore put more emphasis on risk culture. The regulators have a role to play in promoting the correct risk cultures in their jurisdictions. However, regulators may place more emphasis on the quantitative issues of capital and liquidity, frequently at the expense of the no less important qualitative matter of risk culture.[76]

Financial firms are increasing their risk appetite as they search for better returns. The Board and senior management should therefore put more emphasis on risk culture. The regulators have a role to play in promoting the correct risk cultures in their jurisdictions.

The recommended practices included in this handbook under risk culture, risk governance, and balanced incentives programs indicate that, due to the softer qualitative nature of these aspects, the practices to enhance these principles are interrelated and improvement in one area should be combined with others to result in a cascading positive effect across the bank. These include:

- **Board and senior management responsibility.** Effective risk management requires the Board and senior management to take ultimate responsibility for the bank's risk programs. Their role include, setting the right tone at the top, providing adequate resources for the risk management function, developing and determining the design on incentive programs, and facilitating performance evaluation of the

76 Rhodes, W., *Risk culture must change to protect financial system,* Financial Times, 7 August 2014. Available from <http://www.ft.com/intl/cms/s/0/5991c892-19a1-11e4-b-06c-00144feabdc0.html#axzz3B5pIk57e>. [22 August 2014].

Board, senior management, and the bank's employees against predefined performance objectives

- **The right skills, knowledge, and capacity building.** Those charged with risk management responsibilities must show exceptional knowledge of risk factors facing the bank and the financial services industry in general, to enable them to take a leading role in championing the bank's risk management programs. The bank must also put in place a system which supports consideration of risk management in its hiring practices, induction and continuous training programs to enhance a risk- aware business environment.
- **Incorporation of risk management in key performance indicators** of employees' performance evaluation and incentive programs for promotion, accrual, and payout of the incentive. The extent to which risk culture is embedded in a bank is usually seen through the design and implementation of its incentives programs. Incentives work as a powerful tool in influencing employees' attitude toward a risk-aware culture.
- **Risk management—whose responsibility is it?** A bank should prioritize the establishment of a risk governance structure which lays out the roles and responsibilities of the Board, senior management, risk and control functions, risk champions, business units, and auditors. The clarity on roles and responsibilities will enhance the risk culture and risk governance and effectively a bank's risk management program.
- **Communication** plays an important role in risk management due to its role in providing transparency and reducing ambiguity of a bank's practices. Effective risk culture requires timely, transparent, and honest communication on risks as a way of encouraging risk discussions, while effective risk governance requires that a bank set risk reporting channels to support communication of existing and emerging risks. The success of a bank's incentive program is also influenced by the bank's efforts in creating awareness of the program as a means of gaining support and buy-in from employees and other interested parties such as shareholders.

Effective adoption of the recommended practices included in this handbook should make a significant contribution toward further enhancing the strength and effectiveness of a bank's risk management program. Such a bank will then take a new look at its risk management processes and allocation of resources to ensure that risks are effectively identified, assessed, and managed from strategic planning to day-to-day processes at all levels of the bank.

While it is not possible to completely avoid or predict all risks, a bank that incorporates and considers the soft qualitative factors of risk management plus the quantitative elements is bound to have a long-term competitive advantage in an economically and financially interconnected global environment.

6 Appendix 1: Implementing the Best Practices

This section outlines the various activities that a bank can undertake as it implements the recommended best practices. The bank should note, however, that the processes should be cyclic to continually improve its risk culture, risk governance, and balanced incentive practices.

The following steps should be further customized to the individual setting of the bank to ensure that they achieve the intended objectives of their implementation.

ACHIEVING OPTIMAL RISK CULTURE

A bank trying to strengthen its risk culture should start with an assessment of the current state of its risk culture. This is to understand its current condition and to establish a baseline from which progress and/or improvements in risk culture can be measured.

A bank should aim toward cultural improvement through meaningful changes to its current culture through a three-step process of cultural awareness, cultural change, and finally cultural refinement.

This can be achieved by undertaking the activities indicated in the following stages:

CULTURAL AWARENESS

In the cultural awareness stage, the bank should establish its risk management expectations and define the roles and responsibilities around risk. At this stage, the bank should be communicating clearly and continuously to its employees on what its expectations are.

CULTURAL CHANGE

At this stage, the bank should foster an environment that both recognizes and rewards people for paying attention to risk, including knowing how to challenge the status quo constructively.

The bank can develop motivational systems, both positive and negative, to reward the right kind of behavior or to penalize the wrong kind of behavior. There should be focus on talent management through getting the right people into the right positions to drive the right results, and emphasis on the ethical and compliance standards that are important to the bank.

CULTURAL REFINEMENT

A bank at this stage is getting more experienced and mature at its cultural development and trying to monitor cultural performance versus expectations. The expectations can be set by various stakeholders, including employees, management, and the Board, investors and analysts.

Banks at this stage engage in adjustments of people, strategies and communications in order to produce the cultural outcomes that they desire.

The specific activities undertaken in each stage have been outlined in Figure 6.

ACHIEVING OPTIMAL RISK GOVERNANCE

The process of attaining optimal risk governance starts from the top with the Board and senior management. Whereas many banks may be in different stages of strengthening their risk governance, the process below should be continuous to ensure that the bank is well aware of its complex operating environment, its ever-demanding stakeholders, and the regulatory authorities. This includes:

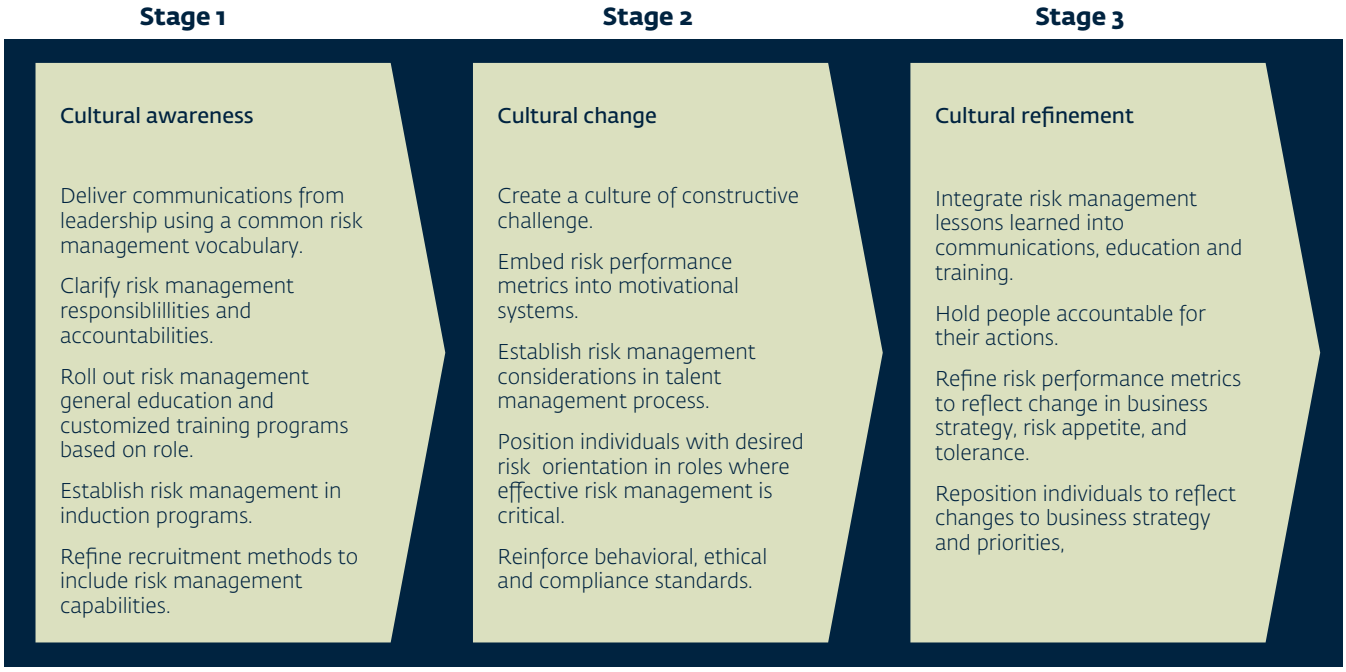
- Developing a risk strategy;
- Defining risk appetite;
- Identifying and assessing risks;
- Aggregating and prioritizing risks;
- Developing action plans; and
- Maintaining vigilance.

DEVELOPING A RISK STRATEGY

This is done by the Board and the senior management and should be done during each strategic planning cycle.

The first activity is for the Board and senior management to make explicit the assumptions on which the strategy is based,

Figure 6: Achieving optimal risk culture



Adapted from Deloitte, *Cultivating a Risk Intelligent Culture* (2012).

and then to constructively challenge those assumptions to test their validity. Once the bank's strategic options are on the table, they should consider the potential interactions among risks that those options might entail, both with respect to individual strategic choices and with respect to different combinations of strategic choices. The Board and senior management will then be in a position to evaluate the risks associated with each strategic option against the bank's risk appetite, short-listing the alternatives that fall within the risk appetite and discarding those that fall outside it.

RISK APPETITE

This is the responsibility of the Board, working with senior management, and should be reviewed at least annually. The risk appetite statement should be cascaded through the various business units.

RISK IDENTIFICATION AND ASSESSMENT

Risk identification, quantification and assessment are important because no effective risk management program can succeed without an in-depth understanding of the specific risks that face the bank. This should be done by the business units at least quarterly or as needed when new risks emerge with the risk function providing the required guidance. Risk identification should go beyond the minimum regulatory standards and not be seen as a simple checklist and "box-checking" exercise.

The information gathered in this process can be consolidated into a report that describes the specific risks facing each part of the bank and their significance and likely directional change. This report can then be reviewed and challenged by the risk function and senior management, who can then aggregate risks across the bank and make adjustments to the bank-wide risks that may not be apparent at a lower level.

RISK AGGREGATION AND PRIORITIZATION

This should be done at least quarterly by the business units, risk function, and senior management. The senior management should include this information in the management reports submitted to the Board.

A "master profile" of risks should be developed for the risks with the greatest consequences to the bank, and a risk dashboard should be created. Senior management should periodically review the status of these risks based on the reports from the business units and the risk management function, and communicate as appropriate with the Board.

DEVELOPING ACTION PLANS

Mitigation actions should be put in place every time a new risk is identified, and such plans should be regularly reviewed by both the business units and the senior management for all the risks facing the bank, as risk management is an ongoing activity.

The Board and senior management should be keen to ensure that any exceeding of limits are promptly identified and rectified and regular revision of the limits are done to respond to any market changes.

MAINTAINING CONSTANT VIGILANCE

The business units, risk management function, and senior management should effectively monitor and report on the risks identified. This would be sufficiently covered by a robust ICAAP process.

ACHIEVING OPTIMAL INCENTIVE PROGRAM

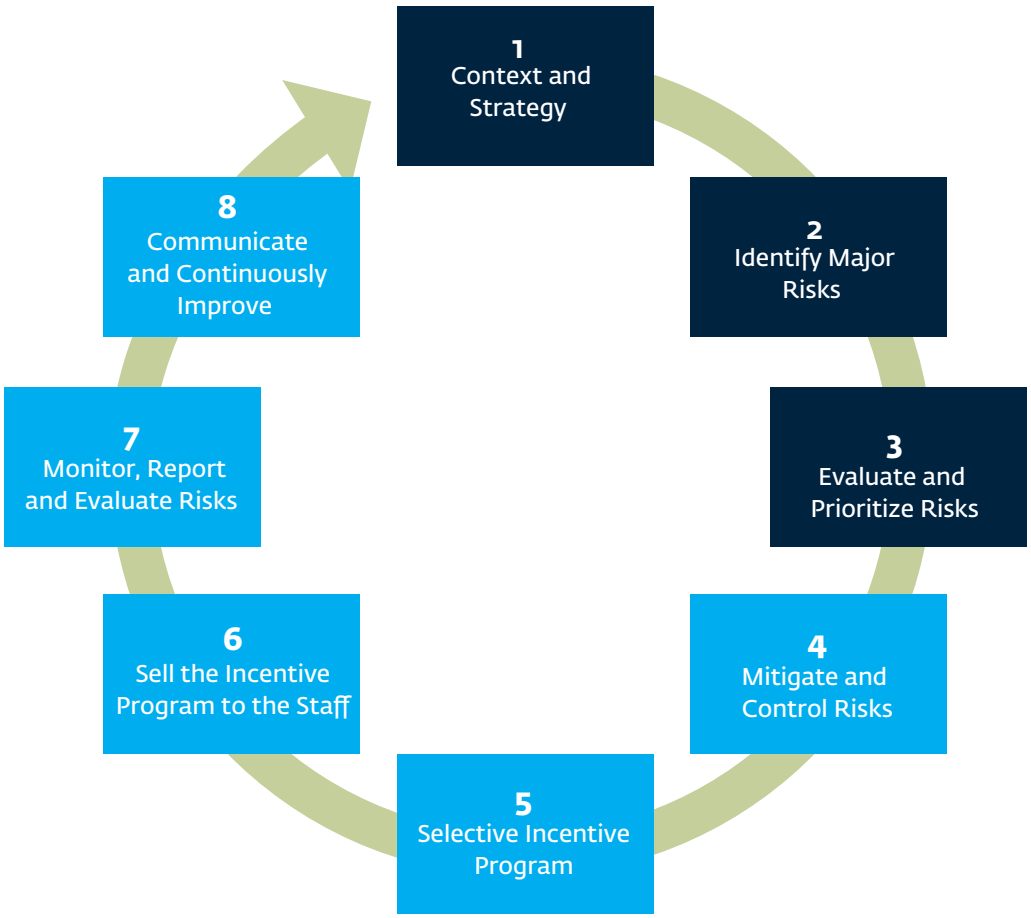
To achieve a balanced incentive program for effective risk management, banks should establish compensation policies that match their risk culture and appetite. These policies and practices should reward appropriate risk taking to achieve an appropriate return and should never reward imprudent risk taking that would affect the bank's solvency or viability.

A holistic approach is recommended to create a good incentive program. This approach calls for an integrated outlook toward a bank's risk management activities which, when implemented, can turn current incentive plans that may be ad hoc or loosely managed into a formal, centrally coordinated incentive compensation program.

Figure 7 illustrates an eight-step approach that can help those charged with design and implementation of incentive compensation programs develop a truly proactive and comprehensive approach to incentive program risks.

The first three steps, in which the compensation team conducts an "Incentive Program Risk Assessment," represent the active process of determining, categorizing, and prioritizing employee incentive program risks. Steps 4 through 8 represent the creation of an "Incentive Program

Figure 7: Achieving a balanced incentive program



Risk Infrastructure" to help mitigate existing risks, implement controls to manage future employee incentive program risks, establish accountability for employee incentive risks and controls, and create a governance structure to monitor risks on an ongoing basis.

STEPS 1-3: CONDUCT AN EMPLOYEE INCENTIVE PROGRAM RISK ASSESSMENT

Step 1 - Understand the Context, Strategy and Objectives behind the Bank's Incentive Program

Defining the incentive program's objectives is a fundamental and important process that requires the participation of the Board and senior management. The objective of the incentive program must be in line both with the strategic goals of the bank and with its culture.[77] The compensation committee or those charged with the incentive program must understand the bank's purpose behind the incentive program in order to manage effectively employee incentives.

With a thorough understanding of the bank's underlying strategy and how the incentives programs support that strategy, the team can evaluate which incentive-related risks may be worth taking, which risks might be less justified, and how risks can be most effectively mitigated or avoided.

Step 2 - Identify Major Incentive Risks and the Functions where the Risks Reside

Risks can only be controlled effectively if one knows where and what they are. We recommend that the bank's compensation committee, with support from other functions such as the risk management, human resources and others as appropriate, compile a complete list of major risks associated with all of the bank's incentive programs and activities and identify the people and departments responsible for controlling each risk. This will provide valuable input for further steps in the risk assessment and ongoing management process.

Step 3 - Evaluate and Prioritize Incentive Risks

A key principle of effective risk management is to distinguish between rewarded and unrewarded risks: Rewarded risks, such as those associated with new product development or new market entry, may be worth taking, but unrewarded risks such as non-compliance or operational failures never are. Depending on the bank's risk tolerance, some risks may be considered minor, others moderate, and still others unacceptably high. The compensation committee's responsibility is to understand the bank's overall risk tolerance, apply the same standards to its list of incentive-related risks, and prioritize the need to mitigate each risk from most to least critical.

STEPS 4–8: CONTINUOUSLY BUILD AN EMPLOYEE INCENTIVE RISK INFRASTRUCTURE THROUGH THE BANK

Step 4 - Mitigate and Control Risks

The functions responsible for various risk identified in step 2 (identification of major risks and functions where the risks reside) are required to make decisions in full consideration of the impact of the identified risks. Their first task should be to mitigate the most critical risks as prioritized in step 3. Once the immediate mitigation controls are put in place, the compensation committee should decide how to institutionalize those processes to mitigate risks on an ongoing basis. This could involve anything from updating the bank's policies and procedures to improving enabling technology to implementing additional controls and oversight over areas where risks are more likely to arise. The important thing is to treat incentive risk mitigation and control as a process that needs to be continued into the near future – not as a simple one-time fix.

Step 5 - Select the Incentive Mechanism

Incentive programs include merit pay, incentive pay, perquisites, benefits, profit sharing, ownership, employee relationship marketing or a combination of these mechanisms. The incentive plans can be further distinguished between short-term and long-term programs as well as between individual and group-based incentives.

Step 6 - Sell the Incentive Program to the Staff

The bank should ensure that staff members understand the incentive programs' mechanics and the reasons for the program. Information on a new or revised incentive program can be communicated through staff emails, newsletters or during meetings of functional areas. Failure to communicate effectively on compensation programs can lead to non-acceptance of the program, which may result in counterproductive impacts on employee motivation.

77 MicroSave, *A Toolkit for Designing and Implementing Staff Incentive Schemes*, 2005, p. 10.

Step 7- Monitor, Report, and Evaluate Risks

This step starts with the review of an ongoing incentive program, in which those charged with regular evaluation of the compensation program regularly monitor risk levels, update, and reprioritize the list of risks. Changes to internal processes, incentive programs, and general business strategy can all have implications for the risks facing the bank and the way in which the department prioritizes and chooses to mitigate them.

Step 8 - Communicate and Continuously Improve

Communication and continuous improvement are the final two components of an effective employee incentive program management infrastructure. By "communication," we mean not just the general need to build a culture that takes risk seriously, but also the need to educate the employees responsible for employee incentive program processes and controls about their specific roles in the risk management process. Each employee who undertakes any form of risk for the bank should know how to execute the correct controls. Such employees should be kept up to date on any changes to those processes and controls. It is also important to be on the alert for opportunities to implement new and improved risk-management tools and strategies as appropriate. As part of the continuous improvement process, the compensation committee may need to undertake a new employee incentive program risk assessment (steps 1 through 3) from time to time as the business environment and the bank's situation change.

7 Working Definitions

Basel Committee on Banking Supervision – This is a forum for cooperation on banking supervisory matters. Its mandate is to strengthen the regulation, supervision and practices of banks worldwide with the purpose of enhancing financial stability.

Board of Directors – This is a group of people who are appointed and/or elected by the shareholders and oversee the running of the bank. It can be either a one-tier Board or a two-tier Board, depending on the country. A one-tier Board delegates its powers to the senior management, whereas the two-tier Boards have a supervisory Board, which oversees the running of the bank, and a management Board, which has the responsibility of running the bank. For this handbook, the Board refers to either the one-tier Board or the supervisory Board.

Business unit – This is a segment of the bank which has a specific function, say human resources, or a branch and is headed by manager. It may be also known as a department, division, or functional area.

Financial Stability Board – This international body was established to coordinate, at the international level, the work of national financial authorities and international standard-setting bodies and to develop and promote the implementation of effective regulatory, supervisory and other financial sector policies in the interest of financial stability.

Incentives – Additional payments given to bank employees on attainment of certain performance measures at the end of a reporting period.

Key performance indicators – A set of quantifiable measures that a bank uses to gauge or compare performance in terms of meeting its strategic and operational goals.

Key risk indicators – A set of quantifiable measures that a bank can use to indicate how risky an activity is. It provides an early warning to identify potential events that may harm continuity of the activity.

Operating management – The team of persons tasked with heading the business units in a bank.

Regulatory authority – This is a public body that is charged with overseeing the activities of commercial banks and is commonly set up to enforce standards. It provides rules, regulations, and guidelines to the banks that operate in its jurisdiction. In some emerging markets, regulatory authorities have prescribed minimum standards for internal controls, risk taxonomies, risk management structure, risk management programs, maximum risk exposures, internal audit programs, and external audit programs.

Risk – The potential for loss or harm, or the diminished opportunity for gain, caused by factors that can adversely affect the achievement of a bank's objectives.

Risk appetite – The aggregate level and types of risk a bank is willing to assume within its risk capacity to achieve its strategic objectives and business plan.

Risk appetite framework – The overall approach, including policies, processes, controls, and a system through which a bank establishes, communicates, and monitors its risk appetite.

Risk culture – The general awareness, attitudes, and behaviors of the bank's Board and employees toward risk.

Risk governance – This is the assessment and management of risks to align risk-taking activities with a bank's capacity to absorb losses and its long-term viability.

Risk intelligence – The ability of a bank to distinguish between two types of risks: the risks that should be avoided to survive by preventing loss or harm; and the risks that must be taken to thrive by gaining competitive advantage. Risk intelligence is the ability to translate these insights into superior judgment and practical action to improve resilience to adversity and improve agility to seize opportunity.

Risk management – The mechanism that creates stability in the bank by enabling the identification, prioritization, mitigation, and measurement of the implications of each decision.

Risk management framework – A structure that supports all processes that the bank undertakes during risk management.

Risk management principles – These are the justifications for carrying out risk management activities. Risk management: creates and protects the shareholders' value; is an integral part of the bank's processes; is part of decision making; explicitly addresses uncertainty; is systematic, structured, and timely; is based on the best available information; is tailored to fit the bank's risk profile; takes into account human and cultural factors; is transparent and inclusive; and is dynamic, iterative, and responsive to change.

Risk profile – A point-in-time assessment of the bank's net risk exposures (after taking into account its mitigating actions) aggregated within and across each relevant risk category based on forward-looking assumptions.

Senior management – A team of persons charged with the responsibility of the day-to-day running of the bank and having the authority to make specific decisions. This will usually include, but is not limited to, the chief executive officer, chief operating officer, chief finance officer, and chief risk officer. They may also be referred to as the senior management.

Tone at the top – The atmosphere that is created in the workplace by the bank's leadership, and that trickles down to all employees.

8 Annexes

ANNEX 1: ILLUSTRATIVE CODE OF CONDUCT

"LIVING OUR VALUES"

[It is advised that the Code of Conduct begin with a leadership letter, which may consist of the answers to some of the following questions: Why does your bank need a Code, and why now? What are some of the challenges that your employees face and how can this Code of Conduct be a helpful document for everyone at all levels? What kind of example might this Code set for others? What are the major trends facing your bank that will impact and affect the Code and its implementation? It is not necessary to address all of the examples. Ideally the leadership letter should be brief and to the point. Like the Code's title—Living Our Values —this letter is meant to inspire.]

STATEMENT OF OUR CORE VALUES

Bank Vision

[Insert bank vision statement]

Principles

[Insert bank principles]

Values

[Insert bank values statement]

Mission

[Insert bank mission statement]

BUILD TRUST AND CREDIBILITY

The success of our business is dependent on the trust and confidence we earn from our employees, customers, and shareholders. We gain credibility by adhering to our commitments, displaying honesty and integrity and reaching the bank's goals solely through honorable conduct. It is easy to say what we must do, but the proof is in our actions. Ultimately, we will be judged on what we do.

When considering any action, it is wise to ask: Will this build trust and credibility for [bank name]? Will it help create a working environment in which [bank name] can succeed over the long term? Is the commitment I am making one I can follow through with? The only way we will maximize trust and credibility is by answering "yes" to those questions and by working every day to build our trust and credibility.

RESPECT FOR THE INDIVIDUAL

We all deserve to work in an environment where we are treated with dignity and respect. [Bank name] is committed to creating such an environment because it brings out the full potential in each of us, which, in turn, contributes directly to our business success. We cannot afford to let anyone's talents go to waste.

[Bank name] is an equal employment / affirmative action employer and is committed to providing a workplace that is free of discrimination of all types from abusive, offensive or harassing behavior. Any employee who feels harassed or discriminated against should report the incident to his or her manager or to the Human Resources department.

CREATE A CULTURE OF OPEN AND HONEST COMMUNICATION

At [bank name] everyone should feel comfortable to speak his or her mind, particularly with respect to ethics concerns. Managers have a responsibility to create an open and supportive environment where employees feel comfortable raising such questions. We all benefit tremendously when employees exercise their power to prevent mistakes or wrongdoing by asking the right questions at the right times.

[Bank name] will investigate all reported instances of questionable or unethical behavior. In every instance where improper behavior is found to have occurred, the bank will take appropriate action. We will not tolerate retaliation against employees who raise genuine ethics concerns in good faith.

For your information, [bank name]'s whistle-blower policy is as follows:

[This policy should be adopted as an addendum to the bank's handbook.]

Employees are encouraged, in the first instance, to address such issues with their managers or the HR manager, as most problems can be resolved swiftly. If for any reason that is not possible, or if an employee is not comfortable raising the issue with his or her manager or HR, [Bank name]'s [Title of Executive Officer] has an open-door policy.

SET TONE AT THE TOP

Management has the added responsibility for demonstrating, through their actions, the importance of this Code. In any business, ethical behavior does not simply happen; it is the product of clear and direct communication of behavioral expectations, modeled from the top and demonstrated by example. Again, ultimately, our actions are what matters.

To make our Code work, managers must be responsible for promptly addressing ethical questions or concerns raised by employees and for taking the appropriate steps to deal with such issues. Managers should not consider employees' ethics concerns as threats or challenges to their authority, but rather as another encouraged form of business communication. At [bank name], we want the ethics dialogue to become a natural part of daily work.

UPHOLD THE LAW

[Bank name]'s commitment to integrity begins with complying with laws, rules, and regulations where we do business. Further, each of us must have an understanding of the bank policies, laws, rules, and regulations that apply to our specific roles. If we are unsure of whether a contemplated action is permitted by law or [Bank name] policy, we should seek the advice of the resource expert. We are responsible for preventing violations of law and for speaking up if we see possible violations.

Because of the nature of our business, some legal requirements warrant specific mention here.

COMPETITION

We are dedicated to ethical, fair and vigorous competition. We will sell [bank name] products and services based on their merit, superior quality, functionality and competitive pricing. We will make independent pricing and marketing decisions and will not improperly cooperate with or coordinate our activities with our competitors. We will not offer or solicit improper payments or gratuities in connection with the purchase of goods or services for [bank name] or the sales of its products or services, nor will we engage or assist in unlawful boycotts of particular customers.

PROPRIETARY INFORMATION

It is important that we respect the property rights of others. We will not acquire or seek to acquire improper means of a competitor's trade secrets or other proprietary or confidential information. We will not engage in unauthorized use, copying, distribution or alteration of software or other intellectual property.

SELECTIVE DISCLOSURE

We will not selectively disclose (whether in one-on-one or small discussions, meetings, presentations, proposals or otherwise) any material non-public information with respect to [bank name], its securities, business operations, plans, financial condition, results of operations or any development plan. We should be particularly vigilant when making presentations or proposals to customers to ensure that our presentations do not contain material non-public information.

HEALTH AND SAFETY

[Bank name] is dedicated to maintaining a healthy environment. A safety manual has been designed to educate you on safety in the workplace. If you do not have a copy of this manual, please see your HR department.

AVOID CONFLICTS OF INTEREST

Conflicts of Interest

We must avoid any relationship or activity that might impair, or appear to impair, our ability to make objective and fair decisions when performing our jobs. At times, we may be faced with situations where the business actions we take on behalf of [bank name] may conflict with our own personal or family interests because the course of action that is best for us personally may not also be the best course of action for [bank name]. We owe a duty to [bank name] to advance its legitimate interests when the opportunity to do so arises. We must never use [bank name] property or information for personal gain or personally take for ourselves any opportunity that is discovered through our position with [bank name].

Here are some other ways in which conflicts of interest could arise:

- Being employed (you or a close family member) by, or acting as a consultant to, a competitor or potential competitor, supplier, or contractor, regardless of the nature of the employment, while you are employed with [Bank name];
- Hiring or supervising family members or closely related persons;
- Serving as a Board member for an outside commercial bank or organization;
- Owning or having a substantial interest in a competitor, supplier, or contractor;
- Having a personal interest, financial interest, or potential gain in any [bank name] transaction;
- Placing bank business with a firm owned or controlled by a [bank name] employee or his or her family; and
- Accepting gifts, discounts, favors or services from a customer / potential customer, competitor or supplier, unless equally available to all [bank name] employees.

Determining whether a conflict of interest exists is not always easy to do. Employees with a conflict of interest question should seek advice from management. Before engaging in any activity, transaction, or relationship that might give rise to a conflict of interest, employees must seek review from their managers or the HR department.

GIFTS, GRATUITIES, AND BUSINESS COURTESIES

[Bank name] is committed to competing solely on the merit of our products and services. We should avoid any actions that create a perception that favorable treatment of outside entities by [bank name] was sought, received or given in exchange for personal business courtesies. Business courtesies include gifts, gratuities, meals, refreshments, entertainment or other benefits from persons or companies with whom [bank name] does or may do business. We will neither give nor accept business courtesies that constitute, or could reasonably be perceived as constituting, unfair business inducements that would violate law, regulation, or policies of [bank name] or customers, or would cause embarrassment or reflect negatively on [bank name]'s reputation.

ACCEPTING BUSINESS COURTESIES

Most business courtesies offered to us in the course of our employment are offered because of our position at [bank name]. We should not feel any entitlement to accept and keep a business courtesy. Although we may not use our position at [bank name] to obtain business courtesies, and we must never ask for them, we may accept unsolicited business courtesies that promote successful working relationships and good will with the firms that [bank name] maintains or may establish a business relationship with.

Employees who award contracts or who can influence the allocation of business, who create specifications that result in the placement of business or who participate in negotiation of contracts, must be particularly careful to avoid actions that create the appearance of favoritism or that may adversely affect the Bank's reputation for impartiality and fair dealing. The prudent course is to refuse a courtesy from a supplier when [bank name] is involved in choosing or reconfirming a supplier or under circumstances that would create an impression that offering courtesies is the way to obtain [bank name] business.

MEALS, REFRESHMENTS, AND ENTERTAINMENT

We may accept occasional meals, refreshments, entertainment and similar business courtesies that are shared with the person who has offered to pay for the meal or entertainment, provided that:

- They are not inappropriately lavish or excessive;
- The courtesies are not frequent and do not reflect a pattern of frequent acceptance of courtesies from the same person or entity;
- The courtesy does not create the appearance of an attempt to influence business decisions, such as accepting courtesies or entertainment from a supplier whose contract is expiring in the near future; and
- The employee accepting the business courtesy would not feel uncomfortable discussing the courtesy with his or her manager or co-worker, or having the courtesy known by the public.

GIFTS

Employees may accept unsolicited gifts, other than money, that conform to the reasonable ethical practices of the marketplace, including:

- Flowers, fruit baskets, and other modest presents that commemorate a special occasion; and
- Gifts of nominal value, such as calendars, pens, mugs, caps and t-shirts (or other novelty, advertising or promotional items) which should not exceed XX amount [nominal value prescribed by the bank].

Generally, employees may not accept compensation, honoraria, or money of any amount from entities with whom [bank name] does or may do business. Tangible gifts (including tickets to a sporting or entertainment event) that have a market value greater than [include monetary amount] may not be accepted unless approval is obtained from management.

Employees with questions about accepting business courtesies should talk to their managers or the HR department.

OFFERING BUSINESS COURTESIES

Any employee who offers a business courtesy must ensure that it cannot reasonably be interpreted as an attempt to gain an unfair business advantage or otherwise reflect negatively upon [bank name]. An employee may never use personal funds or resources to do something that cannot be done with [bank name] resources. Accounting for business courtesies must be done in accordance with approved bank procedures.

Other than to our government customers, for whom special rules apply, we may provide non-monetary gifts (i.e., bank logo apparel or similar promotional items) to our customers. Further, management may approve other courtesies, including meals, refreshments or entertainment of reasonable value provided that:

- The practice does not violate any law or regulation or the standards of conduct of the recipient's organization;
- The business courtesy is consistent with industry practice, is infrequent in nature and is not lavish; and
- The business courtesy is properly reflected on the books and records of [bank name].

SET METRICS AND REPORT RESULTS ACCURATELY

Accurate Public Disclosures

We will make certain that all disclosures made in financial reports and public documents are full, fair, accurate, timely and understandable. This obligation applies to all employees, including all financial executives, with any responsibility for the preparation for such reports, including drafting, reviewing and signing or certifying the information contained therein. No business goal of any kind is ever an excuse for misrepresenting facts or falsifying records.

Employees should inform senior management and the HR department if they learn that information in any filing or public communication was untrue or misleading at the time it was made or if subsequent information would affect a similar future filing or public communication.

Bank's Records

We create, retain and dispose of our bank records as part of our normal course of business in compliance with all [bank name] policies and guidelines, as well as with all regulatory and legal requirements.

All corporate records must be true, accurate and complete, and bank data must be promptly and accurately entered in our books in accordance with [bank name]'s and other applicable accounting principles.

We must not improperly influence, manipulate or mislead any unauthorized audit, nor interfere with any auditor engaged to perform an internal independent audit of [bank name] books, records, processes or internal controls.

Promote Substance over Form

At times, we are all faced with decisions we would rather not have to make and issues we would prefer to avoid. Sometimes, we hope that if we avoid confronting a problem, it will simply go away.

At [bank name], we must have the courage to tackle the tough decisions and make difficult choices, secure in the knowledge that [Bank name] is committed to doing the right thing. At times this will mean doing more than simply what the law requires. Merely because we can pursue a course of action does not mean we should do so.

Although [bank name]'s guiding principles cannot address every issue or provide answers to every dilemma, they can define the spirit in which we intend to do business and should guide us in our daily conduct.

Accountability

Each of us is responsible for knowing and adhering to the values and standards set forth in this Code and for raising

questions if we are uncertain about bank policy. If we are concerned whether the standards are met, or if we are aware of violations of the Code, we must contact the HR department.

[Bank name] takes seriously the standards set forth in the Code, and violations are cause for disciplinary action, up to and including termination of employment.

BE LOYAL

Confidential and Proprietary Information

Integral to [bank name]'s business success is our protection of confidential bank information, as well as non-public information entrusted to us by employees, customers and other business partners. Confidential and proprietary information includes such things as pricing and financial data, customer's names/addresses or non-public information about other companies, including current or potential suppliers. We will not disclose confidential and non-public information without a valid business purpose and proper authorization.

Use of Bank Resources

Bank resources, including time, material, equipment and information, are provided for bank business use. Nonetheless, occasional personal use is permissible as long as it does not affect job performance or cause a disruption to the workplace.

Employees and those who represent [bank name] are trusted to behave responsibly and use good judgment to conserve bank resources. Managers are responsible for the resources assigned to their departments and are empowered to resolve issues concerning their proper use.

Generally, we will not use bank equipment such as computers, copiers and fax machines in the conduct of an outside business or in support of any religious, political or other outside daily activity, except for bank-requested support to non-profit organizations. We will not solicit contributions or distribute non-work-related materials during work hours.

In order to protect the interests of the [bank name] network and our fellow employees, [bank name] reserves the right to monitor or review all data and information contained on an employee's bank-issued computer or electronic device, the use of the Internet or [bank name]'s intranet. We will not tolerate the use of bank resources to create, access, store, print, solicit or send any materials that are harassing, threatening, abusive, sexually explicit, or otherwise offensive or inappropriate.

Questions about the proper use of bank resources should be directed to your manager.

Media Inquiries

[Bank name] is a high-profile bank in our community, and from time to time, employees may be approached by reporters and other members of the media. In order to ensure that we speak with one voice and provide accurate information about the bank, we should direct all media inquiries to the [Public Relations Executive]. No one may issue a press release without first consulting the [Public Relations Executive].

Do the Right Thing

Several key questions can help identify situations that may be unethical, inappropriate or illegal. Ask yourself:

- Does what I am doing comply with the [bank name] guiding principles, Code of Conduct, and bank policies?
- Have I been asked to misrepresent information or deviate from normal procedure?
- Would I feel comfortable describing my decision at a staff meeting?
- How would it look if it made the headlines?
- Am I being loyal to my family, my bank and myself?
- What would I tell my child to do?
- Is this the right thing to do?

INFORMATION AND RESOURCES

Chief Executive Officer (or equivalent)

[Insert name and contact information]

Head of Human Resources (or equivalent)

[Insert name and contact information]

[Title of Other Contact Person]

[Insert name and contact information]

ANNEX 2: ILLUSTRATIVE WHISTLE-BLOWER POLICY

[BANK NAME]WHISTLE-BLOWER POLICY

General

The bank's Code of Conduct requires all employees to observe high standards of business and personal ethics in the conduct of their duties and responsibilities. As employees and representatives of the bank, we must practice honesty and integrity in fulfilling our responsibilities and comply with all applicable laws and regulations.

Reporting Responsibility

It is the responsibility of all employees to comply with the bank's Code of Conduct and to report violations or suspected violations in accordance with this Whistle-Blower Policy (Policy).

No Retaliation

No employee who in good faith reports a violation of the Code of Conduct shall suffer harassment, retaliation or adverse employment consequence. An employee who retaliates against someone who has reported a violation in good faith is subject to discipline up to and including termination of employment. This Whistle-Blower Policy is intended to encourage and enable employees and others to raise serious concerns within the bank prior to seeking resolution outside the bank.

Reporting Violations

The bank's Code of Conduct addresses the bank's open-door policy and encourages employees to share their questions, concerns, suggestions or complaints with someone who can address them properly. In most cases, an employee's supervisor is in the best position to address an area of concern. However, if you are not comfortable speaking to your supervisor or you are not satisfied with your supervisor's response, you are encouraged to speak with someone in the Human Resources Department or anyone in management whom you are comfortable in approaching. Supervisors and managers are required to report suspected violations of the Code of Conduct to the bank's Compliance Officer, who has specific and exclusive responsibility to investigate all reported violations. For suspected fraud, or when you are not satisfied or are uncomfortable with following the bank's open door policy, individuals should contact the Bank's Compliance Officer directly.

Compliance Officer

The Bank's Compliance Officer (or designate) is responsible for investigating and resolving all reported complaints and allegations concerning violations of the Code and, at his/her discretion, shall advise the senior management and/or the audit committee. The Compliance Officer has direct access to the Board Audit Committee and is required to report to the Audit Committee at least annually on compliance activity. .

Matters to Be Reported

Employees may report:

- Any immoral, illegal or unethical practices;
- Violations of the Bank's Code of Conduct;
- Violations of the Bank's accounting procedures or internal controls; and
- [Include the legislations that govern the Bank's practices].

Acting in Good Faith

Anyone filing a complaint concerning a violation or suspected violation of the Code must be acting in good faith and have reasonable grounds for believing the information disclosed indicates a violation of the Code. Any allegations that prove not to be substantiated and which prove to have been made maliciously or knowingly to be false will be viewed as a serious disciplinary offense.

Confidentiality

Violations or suspected violations may be submitted on a confidential basis by the complainant or may be submitted anonymously. Reports of violations or suspected violations will be kept confidential to the extent possible, consistent with the need to conduct an adequate investigation.

Reporting

An employee can use the following channels:

- Through telephone [include numbers – it would help if toll-free lines are available];
- Through fax [include number];
- Through email [include email address];
- Through mail [include postal address and/or physical address]; and
- Through the Bank's website, [include hyperlink to the Bank's website or intranet].

These channels are available throughout the year, and the employee should provide as much information as is possible to enable investigation and resolution of the violation(s) reported.

Handling of Reported Violations

The Compliance Officer will notify the sender and acknowledge receipt of the reported violation or suspected violation within five business days. All reports will be promptly investigated, and appropriate corrective action will be taken if warranted by the investigation.

The possible outcomes of any reports will include any of the following:

- Disciplinary action (up to and including dismissal) and/or legal action against the wrongdoer, depending on the results of the investigation; or
- Disciplinary action (up to and including dismissal) against the employee if the claim is found to be malicious or otherwise in bad faith; or
- No action if the allegation proves unfounded.

ANNEX 3: ILLUSTRATIVE BOARD RISK COMMITTEE CHARTER[78]

I. PURPOSE AND AUTHORITY

The risk committee is established by and among the Board of Directors to properly align with management as it embarks a risk management program. The primary responsibility of the risk committee is to oversee and approve the company-wide risk management practices to assist the Board in:

- Overseeing that the executive team has identified and assessed all the risks that the organization faces and has established a risk management infrastructure capable of addressing those risks;
- Overseeing, in conjunction with other Board-level committees or the full Board, if applicable, risks, such as strategic, financial, credit, market, liquidity, security, property, IT, legal, regulatory, reputational, and other risks;
- Overseeing the division of risk-related responsibilities to each Board committee as clearly as possible and performing a gap analysis to determine that the oversight of any risks is not missed; and
- In conjunction with the full Board, approving the bank's enterprise-wide risk management framework.

The risk committee may have the authority to conduct investigations into any matters within its scope of responsibility and obtain advice and assistance from outside legal, accounting, or other advisors, as necessary, to perform its duties and responsibilities.

In carrying out its duties and responsibilities, the risk committee shall also have the authority to meet with and seek any information it requires from employees, officers, directors, or external parties. In addition, the risk committee should make sure to meet with other Board committees to avoid overlap as well as potential gaps in overseeing the bank's risks.

The risk committee will primarily fulfill its responsibilities by carrying out the activities enumerated in Section III of this charter.

II. COMPOSITION AND MEETINGS

The risk committee will comprise three or more directors as determined by the Board. Each risk committee member will meet the applicable standards of independence, and the determination of independence will be made by the Board. Each member will have an understanding of risk management expertise commensurate with the bank's size, complexity and capital structure.

At least one member will qualify as a "risk expert." The risk committee will consider the experience of the designated member with risk management expertise, including, for example, background in risk management or oversight applicable to the size and complexity of the bank's activities, attitude toward risk, and leadership capabilities.

The risk committee will provide its members with annual continuing education opportunities and customized training focusing on topics such as leading practices with regard to risk governance and oversight and risk management.

Committee members will be appointed by the Board at the annual organizational meeting of the Board. Unless a chairperson is elected by the full Board, the members of the committee may designate a chairperson by majority vote. Additionally, the risk committee, in conjunction with the full Board and with the nominating and corporate governance committee, may do well to consider and plan for succession of risk committee members.

The risk committee will report to the full Board of Directors. The risk committee will consider the appropriate reporting lines for the bank's CRO and the company's management-level risk committee—whether indirectly or directly—to the risk committee.

The committee will meet at least quarterly, or more frequently as circumstances dictate. The committee chairperson will approve the agenda for the committee's meetings, and any member may suggest items for consideration. Briefing materials will be provided to the committee as far in advance of meetings as practicable.

Each regularly scheduled meeting will begin or conclude with an executive session of the committee, absent members of management. As part of its responsibility to foster open communication, the committee will meet periodically with management, heads of business units, the CRO (if applicable) and even divisional CROs, the director of the

78 Adapted from Deloitte, *Risk Committee Resource Guide for Boards, 2012, pp.18 – 21.*

internal audit function, and the independent auditor in separate executive sessions.

III. RESPONSIBILITIES AND DUTIES

To fulfill its responsibilities and duties, the risk committee will:

Enterprise responsibilities

- Help to set the tone and develop a culture of the bank vis-à-vis risk, promote open discussion regarding risk, integrate risk management into the bank's goals and compensation structure, and create a corporate culture such that people at all levels manage risks rather than reflexively avoid or heedlessly take them;
- Provide input to management regarding the bank's risk appetite and tolerance and, ultimately, approve risk appetite and the statement of risk appetite and tolerance messaged throughout the company and by line of business;
- Monitor the organization's risk profile — its ongoing and potential exposure to risks of various types;
- Define risk review activities regarding the decisions (e.g., acquisitions), initiatives (e.g., new products), and transactions and exposures (e.g., by amount) and prioritize them prior to being sent to the Board's attention;
- Review and confirm that all responsibilities outlined in the charter have been carried out;
- Monitor all enterprise risks; in doing so, the committee recognizes the responsibilities delegated to other committees by the Board and understands that the other committees may emphasize specific risk monitoring through their respective activities;
- Conduct an annual performance assessment relative to the risk committee's purpose, duties, and responsibilities; consider a mix of self- and peer-evaluation, supplemented by evaluations facilitated by external experts;
- Oversee the risk program/interactions with management;
- Review and approve the risk management infrastructure and the critical risk management policies adopted by the bank;
- Periodically review and evaluate the bank's policies and practices with respect to risk assessment and risk management and annually present to the full Board a report summarizing the committee's review of the bank's methods for identifying, managing, and reporting risks and risk management deficiencies;
- Continually, as well as at specific intervals, monitor risks and risk management capabilities within the bank, including communication about escalating risk and crisis preparedness and recovery plans;
- Continually obtain reasonable assurance from management that all known and emerging risks have been identified and mitigated or managed;
- Communicate formally and informally with the senior management team and risk management regarding risk governance and oversight;
- Discuss with management and the CRO the bank's major risk exposures and review the steps management has taken to monitor and control such exposures, including the company's risk assessment and risk management policies;
- Review and assess the effectiveness of the bank's enterprise-wide risk assessment processes and recommend improvements, where appropriate; review and address, as appropriate, management's corrective actions for deficiencies that arise with respect to the effectiveness of such programs; and
- In coordination with the audit committee, understand how the company's internal audit work plan is aligned with the risks that have been identified and with risk governance (and risk management) information needs.

Chief Risk Officer

- Ensure that the bank's CRO has sufficient stature, authority, and seniority within the bank and is independent from individual business units within the bank; and
- If the CRO reports to the risk committee, review the appointment, performance, and replacement of the CRO of the bank in consultation of the nomination and governance committee (if applicable) and the full Board.

Reporting

- Understand and approve management's definition of the risk-related reports that the committee could receive regarding the full range of risks the bank faces, as well as their form and frequency;
- Respond to reports from management so that management understands the importance placed on such

reports by the committee and how the committee views their content;

- Read and provide input to the Board and audit committee regarding risk disclosures in financial statements, proxy statements, and other public statements regarding risk;
- Keep risk on both the full Board's and management's agenda on a regular basis; and
- Coordinate (via meetings or overlap of membership), along with the full Board, relations and communications with regard to risk among the various committees, particularly between the audit and risk committees.

Charter review

- Review the charter at least annually and update it as needed to respond to new risk-oversight needs and any changes in regulatory or other requirements;
- Review and approve the management-level risk committee charter, if applicable;
- Perform any other activities consistent with this charter, the bank's bylaws, and governing laws that the Board or risk committee determines are necessary or appropriate; and
- Submit the charter to the full Board for approval.

ANNEX 4: ILLUSTRATIVE TERMS OF REFERENCE FOR A CHIEF RISK OFFICER

BRIEF DESCRIPTION

The Chief Risk Officer (CRO) implements the execution of Enterprise Risk Management (ERM) processes and infrastructure as a key facilitator to achieving the business objectives of the organization with regard to risk and compliance matters.

The CRO will be a member of the senior management of the bank and will be expected to work with the senior management to ensure that the bank's overall business objectives are fully met.

PRIMARY RESPONSIBILITIES

- Assist the Board and senior management to establish and communicate the Bank's risk management principles, objectives and direction to staff;
- Assist the Chief Executive Officer and the Risk Management Committee to develop and communicate risk management policies, risk appetite / tolerance level and risk limits on different corporate activities;
- Implement appropriate risk reporting to the CEO, Risk Management Committee, and full Board;
- Work with management in developing risk mitigation measures to address the bank's key risks and to monitor their effectiveness;
- Establish policies and procedures, risk metrics, risk reports and improvements in risk readiness through communication, training, and risk-based performance management systems;
- Set the strategic risk management vision and deliver that strategy to the bank;
- Facilitate enterprise-wide risk assessments and monitor priority risks across the bank;
- Promote an environment that supports transparency and the bank's key risk-return objectives;
- Implement appropriate systems, controls, and reporting to ensure risk can be managed effectively and in a cost-effective manner;
- As a key member of the senior management team, help develop strategy in a manner that integrates risk management and controls;
- Work with business units to establish, maintain and continuously improve risk management capabilities;
- Work with the Head of Internal Audit and the Chief Finance Officer to ensure alignment between the risk management process and internal audit and risk financing;
- Develop and champion the implementation of an IT strategy to support risk management; and
- Support the development of the risk management team, working as a mentor to direct reports.

DESIRED SKILLS AND EXPERIENCE

- University degree and/or relevant professional qualification;
- Minimum of 15 years' relevant experience in a highly respected bank or financial services organization;
- An intimate knowledge of internal business processes, specifically in the financial services industry;
- A recognized risk leader who is dynamic, proactive and decisive, with the ability to adapt well to and initiate change in the bank, and seek ways to optimize risks as a competitive business advantage;
- Considerable risk management experience;
- Exceptional leadership skills at the executive level;
- High credibility and strong reputation with regulators in the markets he/she has operated in;
- Ability to review and critically analyze substantial amounts of information and bring to bear exceptional decision-making skills; and
- Excellent communication skills, both written and verbal.

ANNEX 5: ILLUSTRATIVE RISK APPETITE STATEMENT[79]

Criteria		Risk Culture
1	Earnings volatility	• Deliver annual target Earnings before Interest, Tax, Depreciation and Amortization (EBITDA) growth of 15% through YYYY. • Maintain a target return volatility of <20% through YYYY (Group level). • Where possible, based on liquidity considerations, retain exposure to real estate market volatility.
2	Target debt rating	• Maintain a large credit rating of AA (stable) or equivalent across external rating agencies.
3	Liquidity headroom	• Maintain a target leverage ratio of 55%, with headroom of $600 MM. • Review earnings at risk monthly to ensure that potential breach of covenants remain <10% of distribution—Take action In the form of financial products If required to mitigate market risk exposures with a focus on FX and commodities.
4	Diversification of levels	• Limit concentration of large exposures to $2 BN of capital in any one country; $200 MM against any one counterparty. • Limit concentration of business unit revenues to 50% of total, and by brand lo 5% of total.
5	Governance	• Ensure operational efficiency and safety standards are maintained within top quartile of industry peer group. • Risk retention and coverage levels (property, liability, business interruption) set to limit potential for catastrophic losses at <1%.
6	Strategy growth	• All new business opportunities to be evaluated on a fully costed, risk-return basis in relation to other investment alternatives. • Strategic options to be considered in light of subsequent portfolio diversification implications.
7	Regulation	• Zero tolerance for any international regulatory breaches. • Exceed legal regulatory standards in key geographies.
8	Corporate reputation	• Maintain a score of >80% on the corporate reputation index (takes into account media, consumer, employee, and analyst views) relative to peer institutions. • Ensure external communications adhere to the highest code of legal standards and transparency within all key markets.

79 Adapted from the Report of the NACD Blue Ribbon Commission on Risk Governance: *Balancing Risk And Reward*, *Appendix C: Developing a Risk Appetite Statement*, published by National Association of Corporate Directors, 2009.

ANNEX 6: ILLUSTRATIVE TRAINING PROGRAM FOR THE BOARD OF DIRECTORS

Training topic	Learning objective	Sample areas to be covered
Introduction to corporate governance	Aim is to provide a background on why corporate governance has grown in prominence and a crucial corporate agenda.	• Why corporate governance is essential for today's Board; and • Background and evolution of corporate governance.
Overview of corporate governance	At the end of the session, the directors will be able to understand the concepts related to corporate governance.	• Corporate governance defined; • Key concepts; • Typical corporate governance structure; and • Key corporate governance actors.
Principles of corporate governance	Objective will be to highlight various best practice and local good practice corporate governance principles such as those issued by key regulators of the financial services industry.	• Principles of corporate governance; • Corporate governance minimum guidelines in the [include region] market. • Board composition and leadership; • Board organization; • Board charter; • Code of ethics; • Independence declarations; and • Delegation of authority and decision-making.
Role in risk management	This aims at sensitizing the Board on what is required so as to ensure that the Board has effective oversight on risk management within the organization.	• Definition of risk and risk management; • Key risks facing the bank and relevant laws and regulations; • Understand the bank's risk management framework, policies, processes, limits; and • How the Board can provide leadership on the risk agenda and drive the Bank toward effective risk management.
Oversight in action—roles and responsibilities	The objective is to sensitize the directors on the roles and responsibilities of the Board so as to effectively carry out their oversight role.	Specific roles of: • Board Chair; • Directors; • Board committees (Audit, Credit, Remuneration); • CEO; • Company Secretary; and • Senior management.
Elevating Board effectiveness	The objective is to highlight how the Board can assure itself on its effectiveness.	• Director induction; • Continued Board education; • Board and Board committees evaluation; • Board succession planning; and • Senior management development and succession planning.

ANNEX 7: ILLUSTRATIVE TRAINING PROGRAM FOR RISK CHAMPIONS

The following is a sample two-day workshop designed for employees who have been identified as risk champions within their business units or the operational managers within the bank. The workshop comprises two sections:

Theoretical Training: This would include the following topics which help the participants to grasp the importance of having risk management be part of each employee's duties:

- Overview of enterprise risk management;
- Recent events that have shaped developments in risk management;
- Why Enterprise Risk Management?
- The process of risk management; and
- Roles and responsibilities in risk management.

Practical Training / Session Breakouts: These assist the participants of the workshop to have hands- on experience on risk issues affecting the bank and include focus groups and exercises that include the following

- Risk identification;
- Risk measurement;
- Risk response; and
- Updating the bank's risk register.

Sample Timetable

Session 1: Introduction to risk management	Session 4: The risk management process – part C
• Purpose of risk management; • Risk management principles; • The risk management process; • Attributes of effective risk management; and • The roles and responsibilities of various stakeholders in risk management.	• Risk treatment; • Risk treatment plans ; and • Risk reporting and assurance. [Breakout session – risk assessment exercise]
Session 2: The risk management process – part A	**Session 5: The risk management framework**
• Establishing the context; • Risk theory; • Risk identification tools; and • Risk description. [Breakout session – risk identification in participants' business units]	• Overview of the risk management framework; • Mandate and commitment; • Monitoring and review; • Continual improvement; and • ICAAP. [Breakout session – going through ICAAP]
Session 3: The risk management process – part B	**Session 6: Good risk management**
• Risk analysis and evaluation; • Qualitative analysis and evaluation; • Awareness of quantitative analysis and evaluation; and • Risk appetite. [Breakout session – role of the risk appetite in achieving the bank's goals]	• How we know when we are doing risk management well; • Being a successful risk manager; and • Achieving a risk-aware culture through successful risk management.

ANNEX 8: ILLUSTRATIVE BOARD RISK COMMITTEE EVALUATION QUESTIONNAIRE[80]

For each of the following statements, select a number between 1 and 5, with 1 indicating that you strongly disagree and 5 indicating that you strongly agree with the statement. Select 0 if the statement is not applicable or you do not have enough knowledge or information to rank the bank's risk committee on that particular statement.

Compostion and quality	1	2	3	4	5
1. Qualified risk committee members are identified by sources independent of management (e.g., independent Board members assisted by an outside search firm).					
2. Members of the risk committee meet all applicable independence requirements.					
3. The designated risk expert meets the definition of "expert" as agreed to by the committee and the Board.					
4. Risk committee members have the appropriate qualifications to meet the objectives of the risk committee's charter, including appropriate risk background/qualifications.					
5. The risk committee demonstrates integrity, credibility, trustworthiness, active participation, an ability to handle conflict constructively, strong interpersonal skills, and the willingness to address issues proactively.					
6. The risk committee demonstrates appropriate banking knowledge and includes a diversity of experiences and backgrounds.					
7. The risk committee participates in a continuing education program to enhance its members' understanding of relevant risk management and banking issues.					
8. The risk committee reviews its charter annually to determine whether its responsibilities are described adequately and recommends changes to the Board for approval.					
9. New risk committee members participate in an orientation program to educate them on the company, their responsibilities, and the company's risk management and oversight policies and practices.					
10. The risk committee chairman is an effective leader.					
11. The risk committee, in conjunction with the nominating committee (or its equivalent), creates a succession and rotation plan for risk committee members, including the risk committee chairman.					
Understanding the business and associated risks	**1**	**2**	**3**	**4**	**5**
12. The risk committee oversees or knows that the full Board or other committees are overseeing significant risks that may directly or indirectly affect the bank. Examples include: • Regulatory and legal requirements; • Concentrations (e.g., suppliers and customers); • Market and competitive trends; • Financing and liquidity needs; • Financial exposures; • Business continuity; • Bank reputation; • Financial strategy execution; • Financial management's capabilities; • Management override of controls; • Fraud control; and • Other pressures such as "tone at the top."					
13. The risk committee discusses the bank's risk appetite and specific risk tolerance levels in conjunction with strategic objectives, as presented by management, at least annually.					
14. The risk committee considers, understands, and approves the process implemented by senior management to effectively identify, assess, monitor, and respond to the bank's key risks.					
15. The risk committee understands and approves senior management's fraud risk assessment and has an understanding of identified fraud risks.					
16. The risk committee considers the bank's performance versus that of its peers in a manner that enhances comprehensive risk oversight by using reports provided directly by management to the risk committee or at the full Board meeting.					

80 Adapted from Deloitte Development LLC, *Risk Committee Resource Guide for Boards*, 2012, pp. 27 – 29.

	Processes and procedures	1	2	3	4	5
17.	The risk committee reports its proceedings and recommendations to the Board after each committee meeting.					
18.	The risk committee develops a calendar that dedicates the appropriate time and resources needed to execute its responsibilities.					
19.	Risk committee meetings are conducted effectively, with sufficient time spent on significant or emerging issues.					
20.	The level of communication between the risk committee and relevant parties is appropriate; the risk committee chairman encourages input on meeting agendas from committee and Board members and senior management, including the CEO, CFO, CRO, CAE, CCO, and business-unit leaders.					
21.	The risk committee sets clear expectations and provides feedback to the full Board concerning the competency of the bank's CRO and the risk function.					
22.	The risk committee has input into the succession planning process for the CRO.					
23.	The agenda and related information (e.g., prior meeting minutes, reports) are circulated in advance of meetings to allow risk committee members sufficient time to study and understand the information.					
24.	Written materials provided to risk committee members are relevant and at the right level to provide the information the committee needs to make decisions.					
25.	Meetings are held with enough frequency to fulfill the risk committee's duties at least quarterly, which should include periodic visits to bank locations with key members of management.					
26.	Regularly, risk committee meetings include separate private sessions with business unit leaders, the CRO, and the CAE.					
27.	The risk committee maintains adequate minutes of each meeting.					
28.	The risk committee meets periodically with the committee(s) responsible for reviewing the bank's disclosure procedures (typically the audit committee) in order to discuss respective risk-related disclosures.					
29.	The risk committee coordinates with other Board committees (e.g., audit committee) to avoid gaps or redundancy in overseeing individual risks.					
30.	The risk committee respects the line between oversight and management of risks within the organization.					
31.	Risk committee members come to meetings well prepared.					
	Monitoring activities	**1**	**2**	**3**	**4**	**5**
32.	An annual performance evaluation of the risk committee is conducted, and any matters that require follow-up are resolved and presented to the full Board.					
33.	The bank provides the risk committee with sufficient funding to fulfill its objectives and engage external parties for matters requiring external expertise.					
	Communication activities	**1**	**2**	**3**	**4**	**5**
34.	The risk committee communicates regularly with regulators and others on risk- management-related matters.					

9 References

Accenture. 2013. *Global Risk Management Study.*

Alessi, C., Sergie, M.A., Understanding the Libor Scandal <http://www.cfr.org/united-kingdom/understanding-libor-scandal/p28729> 5 December 2013 [viewed on 11 November 2014]

Ashby, S., Palermo, T., & Power, M. 2012. *Risk culture in financial organizations: An interim report.* The London School of Economics and Political Science.

Bank for International Settlements. 2010. *Principles for enhancing Corporate Governance.*

Basel Committee on Banking Supervision. 2011. *Range of Methodologies for Risk and Performance Alignment of Remuneration.*

Basel Committee on Banking Supervision. 2010. *Principles for Enhancing Corporate Governance.*

Board of Governors of the Federal Reserve System. 2011. *Incentive Compensation Practices: A Report on the Horizontal Review of Practices at Large Banking Organizations.*

Brodeur, A., Buehler, K., Pastalos-Fox, M., & Pergler, M. 2009. *The Role of the CRO: Risk Management Lessons from the Crisis. McKinsey & Company.*

Campbell, A., Cultural failures at JP Morgan, Barclays and HBOS. Available from <http://www.risk.net/operational-risk-and-regulation/feature/2266779/cultural-failures-at-jp-morgan-barclays-and-hbos/page/3>. [22 August 2014] [viewed on 22 August 2014].

Chibayambuya, J. and D.J. Theron. *The Application of Holistic Risk Management in the Banking Industry.* University of Johannesburg.

Commission of the European Communities. 2009. *Commission recommendation on remuneration policies in the financial services sector.* Brussels. C (2009) 3177.

Commission of the European Communities. 2005. Commission Recommendation complementing Recommendations 2004/913/EC and 2005/162/EC as regards the regime for the remuneration of directors of listed companies.

Committee of Sponsoring Organizations of the Treadway Commission. 2004. *Enterprise Risk Management - Integrated Framework.*

Deloitte. 2006. The Risk Intelligent Enterprise: ERM done right.

Deloitte. 2008. Less risk, greater rewards: Taking a risk intelligent approach to your employee rewards program.

Deloitte. 2009. *Altering Compensation Approaches to Reflect the Changing Financial Services Landscape.*

Deloitte. 2012. Cultivating a Risk Intelligent Culture: Understand measure, strengthen, and report.

Deloitte. 2012. Risk Committee Resource Guide for Boards.

Deloitte. 2012. The Leadership premium: How companies win the confidence of investors.

Deloitte. 2013. Culture in banking: Under the microscope.

Deloitte. 2013. Developing an effective governance operating model: A guide for financial services boards and management teams.

Deloitte. 2013. Global Financial Services Industry Risk Transformation Toolkit.

Deloitte. 2013. *Global risk management survey, eighth edition: Setting a higher bar.*

Deloitte. 2014. As risks rise, boards respond: A global view of risk committees

Ernst & Young. 2012. *Progress in financial risk management: A survey of major financial institutions.*

Ernst & Young. 2013. Remaking financial services, risk; Risk management five years after the crisis: A survey of major financial institutions.

Ernst & Young. 2013. Maximizing value from your lines of defense: A pragmatic approach to establishing and optimizing your LOD model.

Ernst and Young. 2014. 2014 Risk management survey of major financial institutions. Shifting focus: Risk culture at the forefront of banking.

European Commission, 2010. Corporate governance in financial institutions and remuneration policies.

European Commission. 2012. Communication to the Commission: Communication from Vice President Šefovi to the Commission on Guidelines on Whistleblowing.

European Confederation of Directors' Associations. 2011. ecoDa's response to the European Commission's Green Paper on corporate governance in financial institutions and remuneration policies.

Financial Services Authority. 2012. *Guidance Consultation: Risks to customers from financial incentives*. London.

Financial Stability Board. 2013. *Thematic Review on Risk Governance, Peer Review Report*.

Financial Stability Board. 2013. Principles for an effective Risk Appetite Framework.

Financial Stability Forum. 2009. *FSF principles for sound compensation practices*.

Goslin, T., & Terry, J. 2008. *The Journal: Global Perspectives on challenges and opportunities*. London: PricewaterhouseCoopers.

L. Hay. 2012, Pearl Meyer & Partners LLC 2012. Trends and issues: Directors' accountability for ensuring risk-based compensation programs.

Institute of Internal Auditors. 2013. IIA Position Paper: The three lines of defense in effective risk management and control.

Institute of International Finance. 2009. R*eform in the Financial Services Industry: Strengthening Practices for a More Stable System*.

Institute of International Finance. 2010. *Compensation Reform in Wholesale Banking 2010: Progress in Implementing Global Standards*.

International Finance Corporation. 2013. Control Environment Toolkit: Risk Governance, Model Risk Management Committee Charter.

International Finance Corporation. 2012. *Standards on risk governance in financial institutions*.

International Finance Corporation. 2012. *Risk Taking: A Corporate Governance Perspective*.

KPMG International. 2013. *Expectations of Risk Management Outpacing Capabilities: It's Time for Action*.

Levy, C., Lamarre, E., & Twining, J. 2010. *Taking Control of Organizational Risk Culture*. McKinsey & Company.

MicroSave. 2005. A Toolkit for Designing and Implementing Staff Incentive Schemes.

National Association of Corporate Directors. 2009. Report of the NACD Blue Ribbon Commission on Risk Governance: Balancing Risk and Reward.

O'Donnell, S. 2009. *Executive Incentive Practices Post-TARP. Bank Accounting and Finance*.

OECD. 2014, *Risk Management and Corporate Governance*.

Office of the Comptroller of Currency. 2010. The role of a national bank director: The director's book.

Pearl Mayer & Partners LLC. 2012. *Bank Executive & Board Compensation: Compensation Solutions to Reward Today's Directors & Executives*.

PricewaterhouseCoopers. 2009. Risk: Getting appetite right. *PricewaterhouseCoopers, The Journal: Banking and Capital Markets*.

Reserve Bank of India. 2012. Guidelines on Compensation of Whole Time Directors/CEOs/Risk takers and Control function staff, etc.

Rhodes, W. 2014. Risk culture must change to protect financial system, Financial Times, 7 August 2014. Available from <http://www.ft.com/intl/cms/s/0/5991c892-19a1-11e4-b06c-00144feabdc0.html#axzz3B5pIk57e>. [22 August 2014].

The Application of Holistic Risk Management in the Banking Industry," by J Chibayambuya & DJ Theron, University of Johannesburg.

The Association of Insurance and Risk Manager. 2010. *A structured approach to Enterprise Risk Management (ERM)*.

The Incentive Research Foundation. 2012. *Incentives, Motivation, and Workplace Performance: Research & Best Practices*.

United States Federal Law. 2010. *Dodd-Frank Wall Street Reform and Consumer Protection Act*.

Working Group on Corporate Governance - Group of 30. 2012. *Toward Effective Governance of Financial Institutions*.

2121 Pennsylvania Avenue, N.W.
Washington, D.C. 20433
ifc.org