

GOVERNANCE FOR STRENGTHENED RISK MANAGEMENT

GOVERNANCE FOR STRENGTHENED RISK MANAGEMENT

October 2012

PREFACE

THE FINANCIAL CRISIS HIGHLIGHTED WEAKNESSES IN MANY FIRMS IN THE AREA OF RISK GOVERNANCE. RECENT EVENTS INDICATE THAT DESPITE CONTINUED PROGRESS ON REVAMPING GOVERNANCE PRACTICES, ADDITIONAL EFFORTS ARE NEEDED. WHILE THERE IS GROWING CONSENSUS ON WHAT CONSTITUTES SOUND RISK MANAGEMENT AT A TECHNICAL LEVEL, THE GOVERNANCE DIMENSIONS OF STRENGTHENED RISK MANAGEMENT CONTINUE TO BE CHALLENGING.

To address these issues, in 2011 the Institute of International Finance (IIF) established a Task Force on Risk Governance, chaired by Mr. Jacobus (Koos) Timmermans, Vice Chairman of ING. The task force was established under the auspices of the Committee on Governance and Industry Practices (CGIP), chaired by Mr. Richard Waugh, President and CEO of Scotiabank and Vice Chairman of the IIF Board of Directors.

The work of the task force builds upon the extensive analysis the IIF has developed on governance and Industry risk management practices, including the seminal Final Report of the Committee on Markets Best Practices: Principles of Conduct and Best Practice Recommendations of 2008, and subsequent reports on the implementation of recommendations that include the IIF–Ernst & Young surveys on risk management practices. Previous reports have identified certain weaknesses in risk management practices and lessons to be learned, and developed industry practices to address the weaknesses. Recommendations from the IIF and others have been helpful, and firms continue to work in a focused way to embed them. The present report builds on prior work and aims to provide practical examples of how different firms have successfully approached the implementation of such recommendations.

There is agreement in the industry on the need to build a strong risk culture, develop a robust risk appetite framework, increase the role of the Board and Board risk committees in risk governance and strengthen the role of the Chief Risk Officer (CRO). However, challenges remain in implementing many recommendations on a practical level. Although there is general consensus on the implementation challenges faced by the industry, there is divergence among firms on how to respond to these challenges. There is no quick fix to implementing a strong risk culture or a robust risk appetite framework. Simply mandating the risk governance roles and responsibilities of the Board, its risk committees, and the CRO is unlikely to provide the envisaged improvements in risk management. "One-size-fits-all" requirements that do not take into account a financial institution's corporate governance structure and business model are also less likely to provide meaningful improvements in risk governance than those proportionate to the nature, scale, and complexity of the individual institution.

A financial institution should develop and maintain a risk culture that aligns behavior and compensation policies with its attitude to risk taking and risk management. The belief that "risk is everyone's business" should be ingrained in the day-to-day operation of the institution and a robust risk appetite framework is the best way to achieve this.

In summary, building a strong risk culture, developing a robust risk appetite, and strengthening the roles of the Board, its risk committees, and the CRO are some of the fundamental tenets of strong risk management.

The IIF is releasing this report as a contribution to its members' focused efforts to continue strengthening their governance and risk management frameworks, and to the dialogue with the official sector on these important issues.

The Institute is grateful for the assistance provided by member firms and, in particular, the members of the Task Force who developed this report. The IIF will continue to endeavor to promote strengthened practices in the Industry and foster

constructive dialogue with regulators and policy makers to advance industry practices that contribute to the resilience and stability of the financial sector, and to the performance of the real economy.



Douglas Flint
Group Chairman
HSBC Holdings plc



Charles Dallara
Managing Director
Institute of International Finance



Mr. Jacobus (Koos) Timmermans
Vice-Chairman
ING Bank



Richard Waugh
President and Chief Executive Officer
Scotiabank

TABLE OF CONTENTS

PREFACE	II
TABLE OF CONTENTS	IV
EXECUTIVE SUMMARY	1
INTRODUCTION	5
SECTION 1. RISK CULTURE	7
1.1 Overview	7
1.2 Implementation Challenge - Embedding Risk Culture	9
1.2.1 Example of Practice - Developing Target Risk Culture Behavior	10
1.2.2 Example of Practice - Embedding Risk Culture through a Structured Program	11
1.3 Implementation Challenge - Risk Culture Assessment and Change	12
1.3.1 Example of Practice - Risk Culture Survey	12
1.4 Implementation Challenge - Risk Education	13
1.4.1 Example of Practice - Risk Training	14
1.5 Implementation Challenge - Alignment of Compensation with Risk Governance	15
1.5.1 Example of Practice - Claw Backs	17
SECTION 2. RISK APPETITE	19
2.1 Overview	19
2.2 Implementation Challenge - Linking Risk Appetite and Planning	19
2.2.1 Example of Practice - Linking Risk Appetite and Planning	20
2.3 Implementation Challenge - Cascading Risk Appetite	21
2.3.1 Example of Practice - Choice Modelling	22
2.4 Implementation Challenge - Developing Risk Metrics	22
2.4.1 Example of Practice - Developing Metrics	24
SECTION 3. ORGANIZATIONAL STRUCTURES - ROLE OF THE BOARD AND BOARD RISK COMMITTEES	26
3.1 Overview	26
3.2 Implementation Challenge - Strengthening Board Risk Committees	27
3.2.1 Example of Practice - Board Risk Committee Composition	28
3.3 Implementation Challenge - Interaction of Board Risk Committees	29
3.3.1 Example of Practice - The Interaction between Group and Local Boards	30
3.4 Implementation Challenge - Risk Reporting to the Board	30
3.4.1 Example of Practice - Risk Reporting	31
3.5 Implementation Challenge - Use of Stress tests and other Key Risk Metrics by the Board	32
3.5.1 Example of Practice - Stress Testing	33
3.6 Implementation Challenge - Board Self-Evaluation	33
3.6.1 Example of Practice - "Top Ten" Board Self Evaluation Checklist	34

SECTION 4. GOVERNANCE AND ORGANIZATIONAL STRUCTURES—ROLE OF THE CRO	36
4.1 Overview	36
4.2 Implementation Challenge - Ownership of Risk	36
4.2.1 Example of Practice Use of Individual Risk-Based Key Performance Indicators (KPIs)	38
4.3 Implementation Challenge - CRO's Role in Decision Making	38
4.3.1 Example of Practice - CRO Veto	39
4.4 Implementation Challenge - Technical vs. Business Expertise	39
4.4.1 Example of Practice - Technical vs. Business Expertise	40
4.5 Implementation Challenge - CRO Role and Reporting Lines	41
4.5.1 Example of Practice - CRO Role and Responsibilities	42
CONCLUSION	43
ANNEX I. ADDITIONAL EXAMPLES OF PRACTICE	44
Section 1. Risk Culture	44
Example 1. Risk Culture Audits – How Do They Work And Are They Effective?	44
Example 2. Risk Culture Audits	46
Example 3. An Example Of Effective Risk Education	47
Example 4. CRO Learning And Training Initiative – Risk Academy	48
Example 5. Risk-Based Compensation Practices	49
Example 6. Compensation Policies To Match Risk Culture And Appetite	51
Section 2. Risk Appetite	52
Example 7. Emerging Risk Identification And Assessment	52
Example 8. Integrating Risk Into The Planning Cycle	53
Example 9. Risk Appetite	54
Example 10. Formally Factoring Risk Into Resource And Budget Planning	56
Example 11. Embedding Risk Appetite In The Organization	56
Example 12. Risk Aggregation	57
Example 13. Linking Risk Appetite To Risk Controls	58
Section 3. Role Of The Board And Board Risk Committees	59
Example 14. Implications Of Two-Tier Board Structure For Risk Committees	59
Example 15. How A Risk Committee Has Been Effectively Strengthened	60
Example 16. Interaction Of The Risk Committee With Other Board Committees	61
Example 17. Interaction Of The Risk Committee With Other Board Committees (E.g., Audit, Credit Risk, Etc.)	62
Example 18. Risk Reporting	64
Example 19. A Management Information System (MIS) Pack That Allows Boards To Assess Risk Effectively	65
Example 20. Role Of Board In Stress Testing	66
Example 21. Role Of Board In Stress Testing	67
Example 22. Board Self-Evaluation Risk Processes	68
Section 4. Role Of The CRO	69
Example 23. Delegation Of Risk Governance Responsibilities	69
Example 24. Formal Statement Of Ownership Of Risk	71
Example 25. Formal Statement Of Ownership Of Risk	72
Example 26. Formal Responsibilities Of A CRO With A Strengthened Role	73
Example 27. CRO Role And Responsibilities	74

ANNEX II. PREVIOUS IIF RECOMMENDATIONS	76
Referenced In Section 1. Risk Culture	76
Referenced In Section 2. Risk Appetite	76
Referenced In Section 3. Role Of The Board And Board Risk Committees	79
Referenced In Section 4. Role Of The CRO	79
IIF BOARD OF DIRECTORS	82
IIF COMMITTEE ON GOVERNANCE AND INDUSTRY PRACTICES	84
IIF RISK GOVERNANCE TASK FORCE	87

EXECUTIVE SUMMARY

In 2008 the Institute of International Finance (IIF) published the *Final Report of the Committee on Markets Best Practices: Principles of Conduct and Best Practice Recommendations* (CMBP report 2008). The CMBP report identified certain weaknesses in risk management practices and lessons to be learned and developed sound industry practices to address weaknesses. Since the CMBP report, the IIF has published several other reports to address improvements in risk governance, including surveys jointly developed with Ernst & Young meant to identify the progress firms are making on the implementation of sound practices. However, although the analytical work and related recommendations have been helpful to firms as they focus on reviewing their practices, challenges remain as firms continue to implement the IIF and other recommendations to strengthen their risk governance practices.

The current report, *IIF Report on Governance for Strengthened Risk Management*, (the Report) tackles some of the gaps between recommendations and their implementation by presenting practical examples of how firms have met key risk governance challenges. It is important to note that this Report is not intended to be a checklist for organizations to follow, but rather it is designed to help senior management in determining how to strengthen risk governance within their firms by providing examples of how individual firms have met implementation challenges. The examples of practice are not mandatory or necessarily best practice, nor appropriate for all firms. In fact, adopting the examples of practice as recommendations might be counter productive, as a rigid, one-size-fits-all approach will prevent firms from adapting practices to their specific nature, scale, and circumstances.

This Report addresses the key implementation challenges faced by firms in implementing recommendations to strengthen 1) *Risk Culture*, 2) *Risk Appetite*, 3) *Role of the Board and Board Risk Committees*, and 4) *Role of the Chief Risk Officer (CRO)*.

In each section, the Report discusses some of the key implementation challenges faced by firms and provides guidance and examples of practice based on practitioners' experience.

1. Risk Culture

Risk culture is identified as a crucial element in strengthening risk governance. It is however, difficult to measure, as it is primarily behavioral. An important message that emerges from the Report is that the "tone at the top" is crucial to building and embedding a strong risk culture. Developing this strong risk culture is a complex undertaking and involves aligning the behavior of individuals with the firm's attitude to risk taking and risk management.

Important steps in establishing and implementing a strong risk culture are likely to include, but not be confined to:

- embedding risk culture at all levels of the organization,
- conducting firm-wide risk assessments or risk surveys that focus on a variety of indicators of risk culture,
- implementing a formal risk education program, and
- aligning compensation with good risk practice.

Embedding Risk Culture

First and foremost, embedding risk culture involves ingraining the belief that "risk is everyone's business." "Hardwiring" desired risk behavior into the firm can be particularly difficult, as such behavior should be seamlessly integrated into governance structures and business processes, and cannot simply be superimposed on existing procedures. Building the desired risk culture can take several years. However, the main challenge is to embed culture deeply in the firm, so that changes in the economic cycle, leadership changes, and staff turnaround do not cause it to fade away.

Conducting Risk Assessments

An institution's culture, including how it relates to risk, is by definition pervasive. While it is easy to "sense" a firm's culture, using objective measures to identify and assess culture is not straightforward. Developing risk culture assessments and, most importantly, deciding what to do with the results, is an area that many firms find challenging – in particular, teasing out actionable results from the "soft" issues likely to arise from any such assessment.

Implementing a Risk Education Program

Education has an important role to play in communicating a clear and consistent attitude toward risk. This involves training not only on the technical aspects of risk, but also communicating the firm's attitude toward risk and expected risk behavior. However, as firms begin implementing a formal risk education program, they quickly realize that this is complex process. Challenging aspects include deciding who to train, how to best deliver the various technical and behavioral aspects of risk training, and how to weave risk into existing training programs.

Aligning Compensation

Compensation policies are one of the key elements of an adequate risk culture. The extent to which risk culture is embedded in an organization can be evidenced by the degree to which compensation policies are risk-based and encourage appropriate behavior. Continuing challenges include designing policies that are truly risk sensitive, providing incentives for the right behavior, and aligning the timing of risk-based compensation with the time horizon of the risk taken. However, the difficulty goes beyond the technical aspects of compensation policies to maintaining the focus on the risk-based elements of compensation as competitive pressures increase.

2. Risk Appetite

A major component of risk governance is the development of a robust risk appetite framework. Risk appetite can provide a consistent framework for understanding risk through the organization and provide a means to ensure that risk considerations are ingrained in the day-to-day operation of the firm.

The joint IIF and Ernst & Young survey results – as well as discussions with firms – indicate that firms are confronting key practical challenges in implementing a robust risk appetite framework. However, three particularly challenging aspects of implementing a risk appetite framework are discussed in the Report:

- linking risk appetite to the planning process and being able to demonstrate a functional link between the two,
- effectively cascading risk appetite through the organization, and
- developing risk metrics, including linking risk appetite to risk limits.

Linking Risk Appetite to the Planning Process

Developing and setting the firm's risk appetite should be integrated into strategic and corporate planning at the beginning of the process. Achieving such integration in practical terms, especially in large and diverse organizations,

can be difficult. Integrating the strategic plan and the risk appetite framework, which have historically had different functions and used differing targets and metrics, is proving challenging for many firms.

Cascading Risk Appetite

Linking risk appetite, actual business decisions, and accountability for those decisions is critical to implementing a risk appetite framework. The organization's risk appetite, tolerance, and risk limits should be defined in a way that is relevant for the business. Staff in the business units should be able to answer the question – “what does risk appetite mean for me?”

Developing Risk Metrics

Organizations need to develop metrics to monitor their risk profile against the stated risk appetite. There should be a consistency of metrics used throughout the firm, yet these must be meaningful and measurable in diverse business units. One issue is the sheer number of risk metrics used to assess risk appetite and the problem of identifying which metrics to use to hold an individual accountable. In many cases, quantitative limits will not be sufficient if the metrics used do not cover all risks, especially such non-financial risks as reputational or legal risk.

3. Role of the Board and Board Risk Committees

The Board and Board risk committees have a critical role in strengthening risk governance that include setting the “tone at the top,” reviewing strategy, and approving the firm's risk appetite. It is the Board that is ultimately responsible and accountable for risk governance. These responsibilities require that Board members and Board risk committees have the appropriate expertise and experience to make rigorous and informed judgments on risk.

Some of the key challenges faced by firms strengthening risk governance and organizational structures discussed in this Report are:

- building strong risk governance committees,
- managing the interaction of various Board and executive risk committees,
- achieving comprehensiveness while maintaining comprehensibility in risk reporting to the Board,
- providing the Board with meaningful stress test results and associated risk analysis to facilitate strategic decision making, and
- conducting Board self-evaluations to assess how the Board fulfills its risk responsibilities.

Strengthening Risk Governance Committees

Increased focus on risk at the Board level can present problems for firms trying to staff a risk committee quickly with directors who have the requisite risk expertise. It can sometimes take time to find Board candidates who combine solid and relevant risk experience with the stature and judgment required to confidently challenge management on risk.

Interaction of Board Risk Committees

Some organizations do not have a single risk committee as such, but instead have various other committees that have responsibility for some aspects of risk oversight. With multiple committees dealing with risk, it is important to consider the danger that risks might fall between the cracks, or that risks are dealt with in silos and their interaction is not properly assessed and considered.

Board Risk Reporting

It is important that the Board be given information that allows it to understand and appreciate risk issues, challenge management on risk decisions, and have a plain-language conversation about risk at the Board level. The biggest risk reporting challenge for many firms is achieving a balance of comprehensiveness and clarity that enables the Board to focus on decision making.

Stress Test Results

Stress testing is used to determine the impact that severe but plausible stresses would have on the firm's balance sheet and financial health. Many firms are still trying to ensure that stress tests presented to Boards facilitate strategic decision making, while simultaneously improving data aggregation and other inputs.

Conducting Board Self-Evaluations

With increased pressure for Boards to take more responsibility for risk governance, it is important that Board members are confident that they are meeting stakeholder expectations, and self-evaluations are one way of accomplishing this. The challenge lies in using self-evaluations as a diagnostic tool to make improvements in Board risk governance practices. Teasing out the root cause of any problems or inefficiencies uncovered requires an objective analysis of the results as well as a willingness by Board members to critically examine their interaction with the firm's management and with each other.

4. Role of the CRO

The CRO is the senior-most officer responsible for risk management in the firm. Since the financial crisis, it has generally been recommended that the CRO have sufficient seniority, voice, and independence from line business management to have a meaningful impact on decision making. It is considered essential that the CRO have direct access to the Board or Board risk committees in some form.

The CRO and the risk function should not be seen as a silo, dealing only with risk and separated from the rest of the business. The CRO should have a strong working relationship with other members of the senior management team, including the Chief Executive Officer (CEO), Chief Financial Officer (CFO), and Chief Information Officer (CIO), as it is this coordination that ensures that risk considerations are taken into account early in the decision-making process. Nonetheless, the foundation of the firm's risk governance should be the premise that the ownership of risk rests squarely with the business.

The key implementation challenges in strengthening the role of the CRO discussed in the Report are:

- ensuring that fundamental ownership of risk resides in the business, not in the risk function,
- defining the CRO's role in decision making,
- deciding on the optimal balance of technical vs. business expertise for the CRO, and
- structuring the CRO's role and reporting line to reflect the organization's governance structure while ensuring the CRO's stature and authority.

Ownership of Risk

Effective risk governance requires that the ownership of risk and accountability for risk are clearly denoted. Regardless of how an organization delineates its risk responsibilities, the guiding principle is that ownership of risk clearly resides with the business. This involves more than putting into place risk governance structures, policies, and procedures. Ingraining the belief that risk is everyone's business requires positive and negative reinforcement of desired risk behavior.

Defining the CRO's Role in Decision Making

It is crucial that the CRO has sufficient status and seniority to influence decision making within the firm. The CRO should have the stature to have an impact on decisions affecting the bottom line. A test of the CRO's seniority and influence on decision making might be to ask when was the last time the CRO's opinion was fundamental in stopping something material from happening or fundamentally changing a core decision.

Balancing Technical vs. Business Expertise

Both technical risk management expertise and a sophisticated understanding of the business are essential for the CRO to effectively influence Board and business decisions. Combining these two characteristics in one person is not easy, and firms may need to strike a balance between the two. Determining the optimal mix and then finding the right person is not always straightforward.

Structuring the CRO's Role and Reporting Line

Different Board structures, business models, and regulatory requirements mean that there is no one model for CRO reporting lines. Due to group structures, matrix reporting lines often are unavoidable. The difficulty lies in ensuring that the CRO has the required access to the Board and senior management to ensure input on risk issues at an early stage in strategic and business decision making.

Conclusion

While it is evident that the industry has made solid progress in improving risk governance standards since the financial crisis, recent events at individual firms indicate that additional efforts are needed to fully embed improved practices. Embedding a strong risk culture is an ongoing process and cannot be accomplished in a short period of time. Ongoing efforts are needed, with constant evaluation to monitor progress made and to assess the challenges that remain. Similarly, putting a robust risk appetite framework into place is an iterative process.

Increasing the risk role and responsibilities of the Board, Board risk committees, senior management and the CRO are areas rightly receiving a great deal of regulatory attention. In addition, building a Board risk committee with directors who combine solid and relevant risk experience with the stature and judgment required to confidently challenge management on risk can sometimes take time, but is worth the effort. Equally, ensuring the stature and independence of the CRO to influence decision making is an ongoing process.

It is important to note that there is no single or uniform approach to improving risk governance, and measures taken should be proportionate to the firm's nature, scale and complexity. Ultimately, aligning the firm's risk governance structure with its broader corporate governance framework and strategy will make for a more robust and lasting improvement in risk management.

INTRODUCTION

The financial crisis evidenced serious failures in the risk governance of a number of firms. Recent events make clear that despite progress in revamping governance practices, additional efforts are needed. While there is a growing consensus on what constitutes sound risk management at a technical level, the governance implications of strengthened risk management continue to be challenging. The industry recognizes that additional work is needed in order to understand the foundations of governance necessary to support robust risk management practices.

Since the 2008 financial crisis, the Institute of International Finance (IIF) and Ernst & Young have produced surveys on progress in financial services risk management¹. Key areas of change since the financial crisis include a substantial increase in the involvement of Boards in risk, including a significant focus on the risk appetite process, and an expansion in the breadth and scope of the Chief Risk Officer's (CRO) responsibilities. Progress also has been made on strengthening risk culture, but it is hard to quickly change organizational culture and even more difficult to quantify those changes.

Ongoing challenges highlighted in the 2012 IIF and Ernst & Young² survey include balancing a sales-driven culture with a risk-control focus, as well as embedding a strong risk culture in the firm. Similarly, developing robust risk appetite frameworks remains a work in progress. Cascading the high-level risk appetite statement through the organization is a particular challenge, as is agreeing on the metrics used to set and monitor risk appetite. Despite the increased involvement of Boards in risk, their specific role and responsibilities are still evolving. One key remaining challenge is how to best report to the Board on risk and how to focus Board members' attention on the most crucial risk factors, especially as Boards and Board risk committees are being asked to digest an increasing amount of risk material. In addition, firms continue to reshape the role of the CRO, ensuring that the risk function has a clear mandate and that the CRO's opinion carries sufficient weight with the business and risk takers.

Despite impressive progress, the recent IIF and Ernst & Young survey indicates that there is still much to be done to fully embed new processes. One IIF member commented that "balancing growth with risk is the challenge"; sustainable growth must be facilitated without compromising risk standards.

With this background in mind, the IIF decided to establish a Task Force to conduct further analysis specifically on strengthened risk management practices within the broader context of organizations' governance.

The objective is provide practical examples based on actual firms' experience and practices that could assist financial institutions as they continue to improve their governance and implement sound risk management practices.

This Report focuses on a number of essential components of risk governance, including risk culture; risk appetite; and the roles of the Board, Board risk committees, senior management, and the CRO. It addresses the essential governance arrangements, structures, and tools required to implement strengthened risk management. This focus is the result of the Task Force's shared understanding that whether the firm's risk governance is sufficiently robust depends on the extent to which a positive risk culture is truly embedded in the firm; whether its risk appetite framework is used to inform decisions on a day-to-day basis; and how its Board, senior management, and CRO exercise their responsibilities in practice.

Private-sector organizations, including the IIF, as well as a number of official-sector bodies, have made numerous recommendations in recent years on governance, risk management, and the strengthening of industry practices³. The focus of this Report is not on reiterating useful recommendations that are already available, but rather on

¹ Institute of International Finance and Ernst & Young, *Making Strides in Financial Services Risk Management*, April 2011; and Institute of International Finance and Ernst & Young, *Progress in Financial Services Risk Management: A Survey of Major Financial Institutions*, June 2012.

² IIF and Ernst & Young, *Progress In Financial Services Risk Management: A Survey Of Major Financial Institutions*, June 2012.

³ See *Final Report of the IIF Committee on Market Best Practices: Principles of Conduct and Best Practice Recommendations*, July 2008 (CMBP report); The IIF Steering Committee on Implementation's (SCI) report, *Reform in the Financial Services Industry: Strengthening Practices for a More Stable System*, December 2009 (SCI report); the Senior Supervisors Group's *Risk Management Lessons from the Global Banking Crisis of 2008*, October 2009; The IIF and McKinsey & Company report, *Risk IT and Operations: Strengthening Capabilities* (Risk IT report), June 2011; Walker, David *A Review of Corporate Governance in UK Banks and Other Financial Industry Entities – Final Recommendations*, November 2009; a joint reports by the IIF and Ernst & Young, *Making Strides in Financial Services Risk Management*, April 2011 (IIF/E&Y Survey), and *Progress in Financial Services Risk Management: A Survey of Major Financial Institutions*, June 2012; and G-30 Working Group, *Toward Effective Governance of Financial Institutions*, 2012. (G-30 Report on Effective Governance).

highlighting some of the fundamental challenges faced by Boards, management, and CROs in implementing sound risk governance in practice.

This Report aims to provide practical examples of how different firms have successfully approached the implementation of such recommendations. The ultimate objective is to provide guidance based on practitioners' experience, to help the industry as a whole to move forward in implementing a robust framework for risk governance.

The areas covered are:

- **Risk culture**, which is the foundation of strengthened risk governance.
- **Risk appetite**, which is a means of translating the organization's attitude and approach to risk into guidance that can be used in its day-to-day operations to underpin decision-making.

- **Role of the Board and Board risk committees**, which are ultimately responsible for risk governance.
- **Role of senior management and the CRO**, as these individuals have a crucial role in disseminating and implementing a robust risk governance framework.

In each area, this Report summarizes generally accepted sound practice recommendations, the main challenges that firms have faced when attempting to implement such recommendations, and practical examples of how firms have addressed these challenges. It should be stressed that experience has shown that it takes time to implement changes, and it is impossible to develop "one-size-fits-all" recommendations to apply to all firms. In fact, such recommendations might be counter-productive as a rigid approach will prevent firms from adapting sound practice to their own specific circumstances. Therefore, implementation of any recommendations on sound practice contained in this Report should be proportionate and relative to the firm's nature, scale and complexity.

IIF member firms that provided Examples of Practice used in this Report include:

- Absa Group Limited
- Allianz SE
- Bank of Montreal
- BNP Paribas
- Commerzbank AG
- Deutsche Bank
- Ernst & Young
- ERSTE Group Bank AG
- FirstRand Bank
- Grupo Santander
- HSBC Holdings plc
- ING Group
- Itaú Unibanco S/A
- JP Morgan Chase
- KBC
- McKinsey & Company
- MetLife
- Nedbank
- Royal Bank of Canada
- Scotiabank
- Suncorp Group
- Swiss Re Ltd
- UBS AG
- UniCredit SpA
- Zurich Insurance Group

SECTION 1. RISK CULTURE

1.1 OVERVIEW

An organization's risk culture determines the way risks are identified, understood, discussed, and acted upon in the organization. A strong risk culture is an essential building block for effective risk governance and is typically seen as heavily dependent on the "tone at the top" and clear and consistent actions by Board members and senior management. Getting risk culture right is fundamental to controlling risk effectively within the organization. It is, above all, about actual behavior – what you do, not just what you say.

While general consensus exists as to what makes up a robust risk culture, recent failures in the culture of individual firms have become apparent. What such failures demonstrate is that embedding and maintaining a robust culture is challenging, firms will need to continue to work hard over a sustained period of time to make substantial progress in this area.

While manifestations of strong and weak risk cultures quickly become apparent, culture is a "soft" concept that is hard to measure and about which it is hard to be objective. It is, however, of such fundamental importance that firms need to make use of all available means to create and maintain a strong risk culture. As the Institute's SCI report⁴ on risk culture makes clear, a firm's culture can be modified over time, and it is the responsibility of each firm's Board and senior management to sustain the necessary effort to achieve a positive result.

Progress toward cultivating a strong risk culture is inevitably measured in years. As the IIF's SCI report indicated, that is especially true when a firm's risk culture needs to be rebuilt after a serious problem has emerged. It is equally true that risk culture requires constant attention; no organization should become complacent in the belief that strong risk culture has been achieved, allowing the Board and senior management to turn their attention elsewhere.

Risk culture is about an organization's attitude toward risk taking and risk management, and it is essentially about behavior. A firm's risk culture cannot be freestanding, it is part of the organization's wider corporate culture. At the least, it needs to be incorporated into such policies as the

firm's Code of Conduct. More significantly, a strong risk culture needs to be integral to the firm's expectations of how its staff conducts its business.

Significant challenges to embedding a robust risk culture exist, but the industry seems to be making progress in addressing them. The recent IIF and Ernst & Young Survey⁵ found that a majority of the firms surveyed were making progress on, or were close to, achieving a strong risk culture. This included strengthening risk roles and responsibilities (69 percent of respondents), improving communication and risk training (67 percent of respondents), and, critically, reinforcing accountability (61 percent of respondents). Making risk everyone's responsibility, including the front-office client-facing businesses, not just the risk function, is an ongoing challenge. This is linked to enforcing accountability in general, and to aligning group risk objectives with those of different businesses and operations in various countries. Some firms highlighted the challenge of cultivating accountability while avoiding a culture of fear. The objective is to have staff feel comfortable discussing risk concerns and flagging potential issues before they become serious problems.

Characteristics of a Strong Risk Culture

Risk culture cannot simply be mandated in an employee Code of Conduct, although the culture a firm wishes to build should be reflected in its policies and procedures. It is manifested in the day-to-day decisions that indicate how risk is identified, understood, discussed, and acted upon. Determining whether a firm's business practices are aligned with its risk culture requires an understanding of the characteristics of a strong risk culture. Deloitte⁶ has done specific work on identifying and defining what they call the Seven Characteristics of a Risk Intelligent Culture, which generally include:

- **Commonality of purpose, values, and ethics** – People's individual interests, values, and ethics are aligned with those of the organization; employees take the firm's stated risk strategy, appetite, tolerance, and approach seriously, and they are motivated to act on or escalate

⁴ On page 31 of the SCI report, risk culture is defined as "the norms and traditions of behavior of individuals and of groups within an organization that determine the way in which they identify, understand, discuss and act on the risks that the organization confronts and the risks it takes."

⁵ Institute of International Finance and Ernst & Young, *Progress in Financial Services Risk Management: A Survey of Major Financial Institutions*, June 21, 2012. (IIF and E&Y report)

⁶ "Deloitte" means Deloitte LLP and its subsidiaries. Please see www.deloitte.com/us/about for a detailed description of the legal structure of Deloitte LLP and its subsidiaries. Eddie Barrett and A.Scott Baret: *Cultivating a Risk Intelligent Culture: understand, measure, strengthen and report*, 2012.

any deviations or other issues that arise.

- **Universal adoption and application** – Risk is considered in all activities, from strategic planning through to day-to-day operations, in every part of the organization.
- **A learning organization** – The collective ability of the organization to manage risk more effectively is continuously improving.
- **Timely, transparent, and honest communications** – People are comfortable talking openly and honestly about risk, using a common risk vocabulary that promotes shared understanding.
- **Understanding of the value of effective risk management** – People understand, and enthusiastically articulate, the value that effective risk management brings to the organization.
- **Responsibility – individual and collective** – People take personal responsibility for the management of risk, and they proactively seek to involve others when that is the better approach.
- **Expectation of challenge** – People are comfortable challenging others, including authority figures, and the people challenged respond positively.

Inherent within each of these characteristics is the understanding that they ought to permeate the firm's day-to-day business practices. Firms with strong, clear, and pervasive risk cultures can operate with more confidence that their employees' decisions are aligned with, will adhere to, and will support the firm's risk management philosophy.

On the other hand, as recent events have demonstrated, any firm lacking some or all of these characteristics may witness the effects of this cultural weakness directly in its decision-making and business practices. Failing to have a strong risk culture in place to drive business practices can have significant consequences for the firm, affecting its bottom line and generating reputational, compliance, regulatory, and supervisory issues.

Failure of Risk Culture

Useful analysis has been done on failures of risk culture and some common risk culture failure modes have been identified. The SCI report report states that risk culture failings tend to fall into some relatively predictable categories:⁷

- **Disregard for risk:** people make conscious decisions to disregard their firm's risk appetite or its stated norms.
- **Sweeping problems under the carpet:** the culture may or may not induce people to face up to problems as they develop.

- **Passivity:** as most people have jobs to do that focus on specific tasks, they may not react to signals of developing risk unless they are specifically tasked to focus on risk issues.
- **Ignorance:** a lack of understanding of risk management issues or a rote approach that does not induce critical responses.
- **Failure to correct bad behavior:** people within a culture are highly sensitive to signals and reactions to bad behavior.

McKinsey has identified four types of risk culture failure that have tripped up numerous organizations over the decades⁸.

The first is **denial**, a "head in the sand" approach to recognizing and surfacing risks. Signs include overconfidence, in which management and businesses believe that their organizations are immune to pitfalls plaguing peers. Denial often also includes low challenge or a fear of bad news, in which senior management is so committed to a communicated result in terms of business or risk performance that bad news is suppressed.

A second failure mode is **detachment**, in which risk issues are not understood or acted upon promptly. Such detachment could be underlying either an organization encumbered by excessively complicated escalation processes or indifference that undermines swift action. Indifference and detachment also can manifest themselves in lack of rigor, where risk issues are reported and debated at a perfunctory or superficial level, but not analyzed or debated in depth, or pursued to assure resolution.

The third failure mode is a culture of **ambiguity**, in which organizations operate with poor information or insight into their risk profile. These organizations also might have risk definitions or limits that are either not widely understood or that are seen as negotiable. Examples include risk models that are perceived to be immature, irrelevant, or not stable, and, as a consequence, are frequently overridden, or risk reporting that includes only net exposures or is set at too high a level to signal emerging problems. Part of the problem may be the result of under-investment in the risk function, in risk processes, or risk IT.

The fourth and often worst failure mode is a **disregard for risk and active exploitation of loopholes** in the risk system that result in gaming and attempts to beat the system. Some cultures tend to celebrate leaders who "get things done" which, at times, can extend into a culture of pushing boundaries, getting around approvals, or disregarding controls. Excessive internal competition between business units or teams also can lead to a disregard

⁸ Cindy Levy, Eric Lamarre, and James Twining, *McKinsey Working Papers on Risk - Taking Control of Organizational Risk Culture*, Number 16, February 2010.

⁷ SCI report, AIII.4 – AIII.5

for risk in the form of not sharing key information or not actively helping to avoid risk pitfalls in other areas. This has been partially addressed in some firms by increasing the status of the CRO and the risk function (as discussed in the CMBP report and in the IIF and Ernst & Young Survey) in line with official and industry regulations, but the danger of a strong front-office or trading function with the ability to disregard or get exceptions to risk policies until a problem gets out of control is shown by many of the firm-specific issues that have become public.

Important steps in establishing and implementing a strong risk culture are likely to include, but not be confined to:

- embedding risk culture at all levels of the organization,
- conducting firm-wide risk assessments or risk surveys that focus on a variety of indicators of risk culture,
- implementing a formal risk education program, and
- aligning compensation with good risk practice.

1.2 IMPLEMENTATION CHALLENGE – EMBEDDING RISK CULTURE

Building a strong risk culture involves aligning behavior with the firm's attitude toward risk taking and risk management. First and foremost, embedding risk culture involves ingraining the belief that risk is everyone's business. "Hardwiring" desired risk behavior into the firm can be particularly difficult, as such behavior should be seamlessly integrated into governance structures and business processes, and cannot simply be superimposed on existing procedures. Building the desired risk culture can take several years. However, the main challenge is to embed culture deeply in the firm so that changes in the economic cycle, leadership changes, and staff turnaround do not cause it to fade away. Ongoing efforts are a must to maintain a strong risk culture.

The Tone at the Top

The attitude of senior management, or the "tone at the top," is key to getting risk culture right. In conjunction with the Board, senior management, including the Chief Executive Officer (CEO), should develop and outline a clear vision of the firm's approach to risk and risk culture and ensure that structures, responsibilities, and compensation arrangements reinforce this vision. Risk considerations should visibly underpin strategic and resource allocation decisions. Above all, it is crucial that the Board and senior management visibly and continuously demonstrate a commitment to a strong risk culture through their actions and communication. The organization will take its cues from management, and leaders who visibly value a strong risk culture will have a good chance of developing one.

Conversely, management that only gives lip service to sound risk culture values or frequently overrides risk constraints will give the opposite signals and undermine any progress achieved.

Risk in Decision Making

An element of embedding risk culture is to ensure that risk considerations are explicitly highlighted in critical strategic decision processes, for example, decisions on acquisitions, new product development, or IT investment. This should include a thoughtful discussion and analysis of potential risks and requirements to monitor, manage, or control those risks. The process should be designed to give assurances to the Board that risks are understood, are within the firm's risk appetite, or are reflected in an explicit modification of its risk appetite and can be managed with existing IT and human resources. If not, there should be a plan to manage or mitigate them. Major decisions generally will require demonstrable commitment of senior management time to analyze risk implications of those decisions.

Robust risk governance process and policies should be part of the decision-making process to make sure risk issues, risk mitigants, and the costs of accepting or managing risk are taken into account. Ad-hoc or rushed processes that may enable businesses to avoid the risk implications of their decisions should be avoided. Assessing the risk considerations of any business decision should become as fundamental as analyzing the its financial implications.

Challenge Culture

As part of a healthy risk culture, members of senior management should demonstrate that they are willing to be challenged on the basis of the risk framework, and to challenge others. It is important that the Board be given information that allows it to challenge management on risk decisions. The objective is to have a plain-language conversation about risk. This conversation at the Board level should not simply include line management, but also should be actively led by the business.

Staff should be encouraged to raise potential risk issues and provided with the appropriate channels to do so. The opportunities, even the requirement, to raise risk issues should be built into committee structures and mandates, and hardwired into business processes and procedures. Constructive challenge should be welcomed and rewarded at all levels. Challenge and other elements of behavior expected in a positive risk culture should be an important element of the regular staff evaluation process.

Response and Reinforcement

To reinforce desirable risk behavior, it is important to have a predictable and consistent response to breaches of limits and other aspects of non-compliance with established risk parameters. Material breaches should be escalated to appropriate levels and all relevant staff should be aware of this process. One approach is to report on all portfolios on a regular basis using common metrics. In this way, portfolios that require attention are identified quickly and consistent and granular reporting ensures transparency. This ensures that bad news invariably reaches the top of the organization, so staff is more likely to raise problems sooner on their own. Getting the balance right between taking resolute action, while not encouraging concealment of non-compliance can be difficult, but is extremely important in reinforcing appropriate risk behavior.

Bright Lines

To embed the organization's risk culture, clarity about what constitutes unacceptable reputational or legal risks is needed. There should be a wide understanding that many transactions or patterns of transactions may subject the firm to potential legal or operational risk. Those staff who make decisions that raise legal questions or doubts about operational capacities should understand the need to seek expert advice internally before committing the firm. Staff dealing with customers should have a clear understanding of the firm's policies with respect to fair treatment and complaints.

1.2.1 Example of Practice – Developing Target Risk Culture Behavior

One approach to developing target risk culture behavior used by one bank is to first research risk incident reviews that may indicate root cultural issues. Once desired risk culture norms are articulated and root cultural issues identified, critical processes can be screened to assess which ones require attention to foster alignment with the target risk culture. It may be effective to identify routine processes that indicate successful embedding of desired risk behavior, and then integrate these into regular risk culture assessments.

The process of researching risk incident reviews can be a powerful diagnostic tool. Once desirable and undesirable patterns of behavior are identified (and, if possible, relevant metrics identified), a case can be made for changes to front-office processes if risk culture weaknesses have been identified. The objective should be to identify the "moments of truth" in businesses processes, new product approval, or sign-off of high-materiality trades that signal the need for change. Demonstrating that moment of truth signs of weakness exist in a given business can have a meaningful impact on embedding desired risk culture behavior.

Finally, once identified, changes should be hardwired into processes and procedures, for example, by requiring approval sign-offs, reducing tolerances for data problems or delays, or escalating breaches of limits. Such procedural changes should be supported by relevant Management Information Systems (MIS) reporting to make sure that the metrics that have been identified are monitored regularly, significant changes are reported and escalated, and management at each level takes action to correct problems or, where appropriate, to seek changes in the firm's risk appetite.

Examples of routine practice changes intended to embed the target risk culture could include:

- **New product approval:** augmenting the process to embed heightened rigor and reflection on the infrastructure consequences of new products or businesses in terms of expected cost and potential variance and potential operational risk-driven events.
- **Trade approval:** amending the process for high-risk or high capital-intensive structured trades to lift trades with a threshold of materiality out of the routine sign-off process into a review forum with cross-business, cross-functional dialogue.
- **Reputational risk governance:** enhancing the framework to allow multiple business or function leaders to escalate a reputational concern on any transaction or credit into a front-office, chaired forum with mandatory cross-business challenge.
- **Look back MIS:** enriching business-level performance data to provide more insight into data indicative of such risk culture vulnerabilities as infrastructure cost overruns and error rates in the front office that may drive up operational risk or capital calculation errors.

Monitoring Risk Culture

Risk culture is difficult to measure and quantify; however, efforts should be made to monitor the extent to which it is embedded in the day-to-day operations of the firm. In its 2012 report *Progress on the Risk Governance Journey, but Key Challenges Remain*, Ernst & Young and Tapestry Networks⁹ suggested some measures to monitor risk culture. These include tracking:

- the number and frequency of broken risk limits,
- causes of limits being exceeded,
- the number of problems identified in internal audit reports,
- the manner in which audit problems were addressed,
- the percentage of self-reported risk problems,
- the degree to which information is filtered as it is escalated, and
- how the firm deals with staff who have violated risk policy, including how unintentional mistakes are addressed.

1.2.2 Example of Practice – Embedding Risk Culture through a Structured Program

One approach to embedding risk culture used by one bank is to implement a structured program that includes the following elements:

- **Articulation of expected behavior:** defining core risk cultural behavior introduced through a series of tone from the top messages.
- **Ongoing communication:** regular, ongoing communication of core behavior through tone from the top messages, internet, and poster campaigns.
- **Training:** conducting a gap analysis by developing consistent bank-wide general risk awareness training, with specific modules adapted to different staff levels, including promotions to senior positions and new staff.
- **Accountability and measurement:** integrating risk culture behavior into performance management systems and including risk culture behavior in employment contracts and key compliance policies (for example, the Code of Business Conduct and Code of Ethics).

These elements address several of the characteristics of a strong risk culture, including clearly setting expectations, communicating these expectations through various channels, and holding individuals responsible for their risk behavior.

Although behavior is not easily measured, firms can use certain metrics to look for evidence of adherence to the desired traits of the risk culture they want to cultivate. Defining metrics to assess adherence to core risk culture behavior can be especially challenging, but it is crucial. Employee surveys are an additional tool that also should be leveraged to provide information on progress embedding the right risk behavior.

Key risk indicators can be defined and measured at the general staff and senior management levels to identify any red flags; that is, any breaches or examples of non-compliance with core risk culture behavior that can be noted and tracked. These red flags should cover the full range of non-compliant risk behavior, including such cultural issues as failure to comply with hiring or human resources procedures, ignoring required risk vetting or clearances, or technical breaches of limits. Some examples of red flags include:

- trade breaches,
- failure to complete mandatory training,
- failure to complete mandatory time away,
- failure to meet or delays in meeting data-input requirements,

⁹ Tapestry Networks and Ernst & Young, *Progress on the Risk Governance Journey, but Key Challenges Remain*, Bank Governance Leadership Network – Viewpoints. January 12, 2012.

- failure to meet data quality requirements,
- failure to meet documentation requirements, and
- failure to meet compliance requirements.

1.3 IMPLEMENTATION CHALLENGE – RISK CULTURE ASSESSMENT AND CHANGE

An institution's culture, including how it relates to risk, is by definition pervasive. While it is easy to "sense" a firm's culture, using objective measures to identify and assess culture is not straightforward. Developing risk culture assessments and, most importantly, deciding what to do with the results is an area that many firms find challenging; in particular, teasing out actionable results from the "soft" issues that are likely to arise from any such assessment.

Risk Culture Surveys

Organizations should take all practical steps to ascertain that risk culture is understood and embedded within the firms should use all evidence-based means at their disposal to assess existing strengths and weaknesses, identify areas for improvement and monitor progress when the need for change is identified.

One way firms can do this is by conducting risk assessments or risk surveys. This can be either a focused exercise or part of a broader survey of employee attitudes and opinions. Staff at all levels should be asked to speak freely about their understanding of the organization's risk culture and how it affects their jobs. Their ability and willingness to speak freely will in itself be an important indicator of the adequacy of the culture in the firm.

The primary objective of risk culture surveys is to understand attitudes to risk and identify gaps and potential problem areas. Risk culture surveys should be repeated at regular intervals to assess progress in remedying any problems. One of the more critical uses of a risk culture survey can be to help develop an action plan to implement needed changes identified on the basis of survey results.

1.3.1 Example of Practice – Risk Culture Survey

When a formal audit or survey of risk culture issues is undertaken, questions should go beyond whether the risk culture is understood to how it works in practice, and whether it is perceived to be strong or weak. Specifically, questions should attempt to get at the individual employee's experience of the firm's risk culture, rather than only asking about general perceptions of the culture.

A common approach to survey risk culture¹⁰ used by many firms is to present a series of statements and ask staff to rate how strongly they disagree or agree on a scale of one to five. Such a survey may focus on both organizational and individual factors. Some sample questions included in this type of survey are:

Organizational Factors

Communication: The section attempts to ascertain if communication is frequent and effective, and sets clear expectations.

- Is there a clear and coherent strategy for managing risks in the business?
- Does the firm's leadership set clear expectations for risk behavior?
- Do policies and procedures support effective risk management?

Resources: Resource statements focus on whether the firm provides adequate resources and training on risk.

- Does the organizational structure allow staff to manage risk?
- Are there clear guidelines and requirements for risk reporting and escalation?
- Is risk management training effective for the employee's role?

¹⁰ Ernst & Young, *Risk Culture in Financial Services*, July 2012.

Incentives: Staff is asked to rate the degree to which they are provided with feedback and rewarded to encourage appropriate risk behavior.

- Are employees rewarded for adherence to risk behavior?
- Are employees held accountable for noncompliance to risk policies or procedures?
- Are there meaningful consequences for not adhering to risk policies?

Individual Factors

Competencies: This section is aimed at rating whether staff understand the risk skills required in their job.

- Do colleagues have the right skill level for effective risk management?
- Does the firm learn from past mistakes?
- Are the employee's required skills and competencies clear?

Application: This section focuses on whether compliance with risk policies and procedures is effectively encouraged in the firm.

- Does management encourage compliance with risk policies and procedures?
- Is risk given appropriate weight and value in decision making?
- Is sharing of information about risk processes encouraged?

Motivation: This section is aimed at testing whether the staff understand the benefits of appropriate risk behavior and if they are comfortable with challenge mechanisms.

- Is the employee committed to the long-term sustainability of the firm?
- Is it important to the employee that the business operates ethically?
- Is it clear to the employee how risk policies reduce risk to the firm?

The results of risk surveys can provide a useful test of whether the firm's risk culture is understood and embedded in the organization. Results can be used as a benchmark to determine where improvement is needed, and then used to check progress when the survey is repeated. The usefulness of risk surveys also can go beyond a management tool to assess risk culture, as many firms share the results with the staff. Firms have found that sharing the results with staff can reinforce transparency and emphasizes the firm's commitment to continuously maintaining and improving risk culture.

Key Risk Indicators

An important goal of any survey should be to identify a set of Key Risk Indicators (KRIs). A risk culture survey can be used to develop KRIs, which may be specific to a particular firm based on, among other factors, its business model or the evolution of its risk culture. They can function as traffic signals; for example, as an amber light indicating that it may be time to step back and more fully examine the risk implications of a business decision. Once identified, KRIs can be used to monitor progress against action plans developed as a result of the risk survey. They also may be incorporated as red flags into the day-to-day management of the business.

The most essential component of an assessment process, based on surveys or other means, is the diagnostic phase when problem areas are detected. The diagnostic exercise should be followed by the development of a specific action plan to address problem areas identified during the survey.

1.4 IMPLEMENTATION CHALLENGE - RISK EDUCATION

Education has an important role to play in communicating a clear and consistent attitude toward risk. Risk education involves training on not only the technical aspects of risk, but also communicating the firm's attitude toward risk and expected risk behavior. However, as firms begin implementing a formal risk education program, they quickly realize that this is complex process. Challenging aspects include deciding who to train, how to best deliver the various technical and behavioral aspects of risk training, and how to weave risk into existing training programs.

Integration of Risk Training

Practical experience has demonstrated that risk education cannot exist in a vacuum. It must necessarily be linked to the firm's values, overall risk governance structure, and risk management framework and procedures. Risk education can inform and sensitize staff to these elements.

Training either risk staff, all employees, or only the members of the Board is a major undertaking, and trade-offs about who to train and what type of education is appropriate for different groups may be required. In deciding which employees to cover, it is important to include as many people as possible, while tailoring training to meet the requirements of different groups. For example, tellers have different training requirements from traders and, in general, those with greater responsibilities need a broader and more specific view of the stakes in risk management.

Whether it is provided by external trainers or in-house, risk training should be integrated into a firm's core training curriculum and included in its leadership, executive, or management training. If training is done by external providers, efforts should be made to include significant senior management input on firm-specific value and culture issues. Practical experience has demonstrated that off-the-shelf approaches are likely to be ineffective, as they are not customized to meet the specific requirements of the firm. Ideally, a member of senior management should be involved in presenting modules dealing with organizational values and corporate culture. The more senior management and the Board can be seen to sponsor training and, within reason, take part in it the better, as this will reinforce the notion of full buy-in within the firm.

1.4.1 Example of Practice – Risk Training

One bank has opted for an approach in which risk training is provided to all members of the staff from director level to tellers. This risk training program emphasizes the firm's values and draws on its Code of Conduct. The focus is on the essential elements of the risk management framework (in essence, how risk is managed in the firm) and on ensuring that risk considerations are ingrained in all day-to-day business decisions. In this firm, risk is not seen as negative. Rather, the core of the firm's approach is that risks must be taken to meet its strategic and business objectives, and such risks must be adequately managed. A responsible attitude to risk taking is encouraged by asking, "What risks will the firm be exposed to in pursuit of its strategic goals?"

This approach to risk is central to the induction training given to all staff. Topics covered include not only the firm's risk management values, but also important elements of risk reporting. Induction risk training can last up to two days, and the CRO, the head of the firm's Enterprise Risk Management (ERM) function, and those in charge of specific risks, such as market risk, help present sessions.

Risk training includes identification, measurement, control, monitoring, and reporting of risk, and policies including escalation procedures and challenge mechanisms, are discussed. One of the key challenge mechanisms is the firm's open-door policy, which encourages any staff member to take risk concerns to a risk manager. The role of risk management and an enterprise risk committee in promoting a challenge culture are equally as important as the more traditional elements of risk management listed above. All staff is introduced to the firm's risk-based Key Performance Indicators (KPIs) during the induction training, further reinforcing the message that risk considerations should be taken into account in the daily operation of the business.

Refresher training is delivered online, and all staff are required to test their knowledge of the firm's values every two years. This test is located on the compliance section of the website and covers broader ethics questions, environmental issues, and money laundering, as well as risk management. There are roughly 20 to 30 questions, and the minimum passing grade is between 80 percent and 90 percent.

Specialist risk training geared to specific roles and areas of the bank also is provided. Unlike induction training, during which staff from different departments attend the same sessions and are taught the same curriculum, specialist training is job-related. Subjects covered could include the risks related to the firm's credit card business or operational risk, depending on the employee's position. Training goes beyond the risk management basics required for the position. For example, credit risk specialist training covers the broader enterprise risk implications of the role in addition to the understanding of credit models.

The ultimate objective of this firm's risk training program is that all staff understand how its approach to risk governance is part of the broader values and ethics of the organization. Staff should have a good awareness not only of overall risk management policies and procedures, but be able to clearly articulate their personal responsibility for risk and how this contributes to organizational risk governance.

Common Language

Perhaps one of the greatest benefits of risk training is the opportunity to create and promote shared understanding about risk based on a common language. This raises awareness of risk and ensures that everyone understands and can communicate the organization's approach to risk. A common language creates a way for staff to describe, deal with, and report on risk in a uniform fashion.

1.5 IMPLEMENTATION CHALLENGE - ALIGNMENT OF COMPENSATION WITH RISK GOVERNANCE

Compensation policies are one of the key elements of an adequate risk culture. The extent to which risk culture is embedded in an organization can be evidenced by the degree to which compensation policies are risk-based and encourage appropriate behavior. Institutionalizing clear repercussions for bad risk behavior and implementing effective mechanisms such as claw-backs are two of the clearest imperatives. However, as practical experience of firms dealing with this issue has demonstrated, crafting a risk-based compensation policy is challenging.

Continuing challenges include designing policies that are truly risk sensitive, providing incentives for the right behavior, and include aligning the timing of risk-based compensation with the time horizon of the risk taken. However, the difficulty goes beyond the technical aspects of designing compensation policies to maintaining the focus on the risk-based elements of compensation as competitive pressures increase.

Aligning Compensation with Risk Culture

A number of regulatory and industry practices have been recommended in the area of compensation policies. In particular, the IIF developed seminal work on industry-wide principles on compensation in the CMBP report, including Principles of Conduct for the design of sound incentive compensation practices by firms. This work was followed by the 2009 joint IIF and Oliver Wyman report, *Compensation in Financial Services*,¹¹ and later reports on *Compensation Reform in Wholesale Banking*¹².

The IIF set of recommendations is aimed primarily at ensuring that firms adequately link risk to compensation policies so that the correct incentives can be established, recommending, for example, that compensation incentives should not induce risk taking in excess of the firm's risk appetite and that payout of incentives should be based on

profit that is adjusted for risk and the cost of capital.¹³ In the SCI report, it was recommended that firms "ensure that compensation schemes incorporate major risk types and account for cost of capital and the time horizon of risks associated with future revenue streams".¹⁴

On the regulatory side the Financial Stability Board (FSB) has outlined guidelines on the effective governance of compensation, effective alignment of compensation with prudent risk taking, and effective supervisory oversight and engagement by stakeholders in its *FSF Principles for Sound Compensation Practices*¹⁵.

Aligning compensation arrangements with desired behavior is a powerful means of reinforcing risk culture. Employees can be given incentives to behave in ways consistent with the firm's risk culture and be penalized when they do not. More fundamentally, the consistent and visible alignment of reward with desired risk behavior sends a powerful signal to staff at all levels about the commitment of the organization's management to maintaining a risk-sensitive culture. Staff should be able to observe a systematic, transparent and, predictable link between how they and others, including senior management behave with regard to risk and how they are rewarded.

However, many practical problems remain in turning this into reality in competitive markets, among them, how to balance positive incentives with penalties. A risk-based approach to compensation can help avoid compensation being driven purely by short-term, market-based considerations. Turning theory into practice involves recognizing both the long-term nature of risk and the fact that taking some risk is necessary to generate a return.

Performance Indicators

It is important that organizations incorporate the long-term challenge of changing behavior with short-term performance when implementing risk-based compensation. Risk-based compensation should be linked to specific performance objectives and, critically, with the firm's risk appetite. Just as good risk behavior, such as constructive challenge of decisions or transactions on the basis of risk criteria should be rewarded, performance measurement or compensation repercussions for breaches of risk limits or failure to conform to expected risk behavior also are required.

It is, however, important to design the means of penalizing bad risk behavior to avoid creating incentives for staff to conceal breaches or to circumvent risk limits without required approvals. A firm's incentives should make

¹¹ IIF and Oliver Wyman, *Compensation in Financial Services: Industry Progress and the Agenda for Change*, March 2009.

¹² IIF and Oliver Wyman, *Compensation Reform in Wholesale Banking 2010: Progress in Implementing Global Standards*, September 2010; and IIF and Oliver Wyman, *Compensation Reform in Wholesale Banking: Assessing Three Years of Progress*, October 2011.

¹³ IIF, *Compensation Reform in Wholesale Banking 2010: Progress in Implementing Global Standards*, 2010, 13.

¹⁴ SCI report, 74.

¹⁵ Financial Stability Forum, *FSF Principles for Sound Compensation Practices*, 2009.

it clear that early identification and escalation of an issue or a mistake is not penalized, whereas failure to raise an issue or give notice of a breach before it is discovered by audit, risk, or compliance is a serious failing.

Individual repercussions for bad risk behavior can range in severity from clear notification thereof, to inclusion in an employee's performance evaluation that may result in a proportionate reduction in bonus or salary, to termination.

Incidents and Consequences Process

One approach to dealing with bad risk behavior is an "incidents and consequences process," whereby control incidents may result in disciplinary action. At one firm, depending on the severity of the individual's infractions, bonuses may be reduced by 10 percent to 50 percent at one level of severity, or 50 percent, and extending to complete elimination of the bonus for a more severe incident. Any variance from this policy has to be formally approved by a high-level, firm-wide review committee, and in the vast majority of disciplinary cases the rules are followed. To put this process into perspective, out of 800 incidents initially evaluated, 200 to 300 were subject to the further review and only approximately half of 1 percent of the firm's employees have been disciplined.

Scorecards

Compensation should be based upon objective indicators, and some firms use tailored scorecards, as more consistent results may be produced when managers are asked to document their thought processes by conducting formal evaluations. A scorecard can help ensure that managers focus on the importance of risk issues.

The use of scorecards can be more problematic in measuring risks taken that might have as yet unrealized reputational and legal implications, which are particularly difficult to quantify unless an incident comes to light immediately. Firms that do not use scorecards may prefer to emphasize judgment and risk identification over metrics, as the latter sometimes do not reveal fundamental aspects of good or bad risk behavior. Another concern raised with scorecards is that they are a lagging indicator. Overall, the use of scorecards is not yet fully evolved, and firms are still exploring how to best incorporate them into their risk-based compensation process.

Repercussions

A common approach to dealing with bad risk behavior is to set up a compliance review committee, which could include members from the risk, compliance, human resources, and audit functions. This is a forum to look at actions that have a material risk impact, and individuals who are brought

before this committee may be subject to disciplinary actions, including a reduction in compensation. The committee's mandate is to review the actions of individuals whose behavior has been flagged as aberrant.

Some examples of bad risk behavior that may result in review are:

- breaches of VaR,
- frequently appearances before the risk committee to explain transactions, trades, or behavioral incidents, and
- noncompliance with limits or thresholds, etc.

Risk-Based Compensation for Risk and Control Functions

One particular challenge is developing risk-based evaluation and compensation policies for the risk, compliance, and other control functions. Bonus pools for risk and control functions should not generally be linked to front-office results. Too strong a link to financial results may provide incentives for risk functions to be overly lenient; however, no link to risk-adjusted results could destroy all risk taking. In practice, the risk function's compensation is typically less sensitive to earnings than that of the front-office staff.

However, in some firms the control functions may be penalized if there is a problem on their watch. Considerations are not just whether the business operated within the risk management framework, but also whether the firm's financial and other targets were met within its risk appetite. The two elements, risk and targets, are equally important; and even if the business made a profit by stepping outside the risk framework, the question of whether the risk function fulfilled its task of identifying, recording, and escalating risk issues is a factor in determining the risk manager's compensation.

It may seem to be counterintuitive that a stellar year of profits for the firm could result in lower compensation for both the risk taker and the risk manager if risk limits and other variables have been violated. However, the relevant risk manager's overall compensation might be decreased if there was material oversight or a failure to rectify risk issues. The consistency of the framework and its predictability are essential elements of a risk-based compensation policy.

Claw Backs

Practical experience with claw backs is evolving. Several firms have implemented claw back processes in accordance with official and industry recommendations, generally enabling claw back of bonuses for periods ranging from two to five years. The length of the claw back period is often dependent on the type of business, as risks in different business lines may take more or less time to emerge.

1.5.1 Example of Practice – Claw Backs

Deferred payouts, typically over one to three years, are often the means of implementing claw backs for senior management and material risk takers. Although it is recognized that the deferral period needs to be long enough for the “tail” risk to materialize, there are often legal constraints on the length of time that a claw back could be exercised, especially for a firm that operates in multiple jurisdictions.

Equity bonuses normally vest over periods of up to three years, whereas risk on certain business lines can take much longer to emerge. Firms have attempted to deal with this divergence in several ways. For credit risk, one option is to avoid paying high bonuses at the top of the cycle, when unrecognized risks are likely to be present in the portfolio, and to avoid giving incentives for “irrational exuberance” that may contribute to bubble behavior, and, conversely, not reduce bonuses to the same extent at the bottom of the cycle. This approach recognizes the need to apply good credit judgment at all stages of the cycle. Another option is to have a lower payout ratio for longer-term risks, although this may effectively penalize individuals who arguably make the most difficult risk decisions. The challenge is to devise ways to risk-adjust bonuses for multiple years’ performance and not simply to reflect short-term risk and current market conditions.

One firm has substantially reduced the front-end bonus payout to result in 20 percent, to 80 percent of the payout deferred to subsequent years. The business rationale is that the firm wants to provide incentives for employees to be more careful with its financial resources by factoring risk considerations into business decisions. Another firm has a two-year claw-back period aligned to the term of its predominant property and casualty insurance business. In this firm, a committee chaired by human resources meets quarterly to assess emerging risks that might be the basis for claw back in the future. These quarterly meetings provide an audit trail for future reference.

However, concerns exist that eventually the enforceability of claw backs will be tested in the courts. For this reason, some firms use alternative measures, considered to be equivalent to claw backs. For example, some firms are of the view that a reduction in compensation for the current year as a result of issues that have emerged from prior-period performance can be more effective. Another method used is to reduce the individual’s management responsibilities as a visible reaction to failure to meet behavioral expectations. A reduction in management responsibility also can have a visible effect within the firm, and can be doubly effective as an incentive as it is likely to be seen as detrimental by potential future employers if the individual chooses to leave the firm. Alternatively, the individual may be required to rectify the problem, or be terminated if that request is refused.

However, aligning claw backs with the time horizon of risk while ensuring enforceability, especially for staff who may have moved to different positions or to another firm, can be difficult.

A recent survey by Mercer¹⁶ indicated that about 17 percent of global banks used claw backs in 2011. The survey found that, prior to 2011, 44 percent of banks had claw back provisions in place, with claw backs being more common in North American banks than at those in Europe, the Middle East and Africa.

Since 2011 a further 18 percent of banks across all regions have introduced claw backs. Mercer noted that claw backs are relatively new, and it could take some time for them to be utilized to their fullest extent.

Deterioration of Risk-Based Compensation Practices

Firms are appropriately concerned about maintaining a competitive pay structure to attract and retain talent. As memories of the last crisis fade and competitive pressures

increase, there is a danger that risk-based compensation practices will deteriorate. Regulators and shareholders will continue to scrutinize compensation going forward, and risk-based compensation may provide a means to avoid the excessive risk taking that often occurs during the financial booms that precede a crisis. It is clear that this issue will remain a priority for human resources and Board compensation committees. In fact, maintaining consistent incentives through risk-based compensation practices over the longer term may be one of the biggest policy challenges faced by human resources.

Procedural Recommendations

A number of actions could be taken to ensure that risk-based compensation retains its relevance and current high visibility. Possible examples of ways to curb imprudent risk taking include:

- transparency and disclosure of risk-based compensation policies,
- including the Board risk and compensation committees in discussions on risk-based compensation policies and requiring their approval for changes,

¹⁶ Ambereen Choudhury, About 17% of Global Banks Clawed Back Compensation, Mercer Says, August 23, 2012. Available at <http://www.bloomberg.com/news/2012-08-23/about-17-of-global-banks-clawed-back-compensation-mercer-says.html>

- institutionalizing risk-based compensation by involving multiple committees and functions, such as risk, finance, compliance, human resources, and audit in setting risk-based compensation, and
- ingraining the expectation that the CRO and the enterprise risk committee provide feedback on compensation, and hardwiring this into the annual pay and bonus process.

SECTION 2. RISK APPETITE

2.1 OVERVIEW

There is general agreement that a robust risk appetite¹⁷ framework is an essential component of an organization's overall risk governance. The report, *Implementing Robust Risk Appetite Frameworks to Strengthen Financial Institutions*,¹⁸ the "IIF 2011 Risk Appetite Report, included a comprehensive review of industry practices and listed a number of recommendations as to how firms could improve their approaches to a risk appetite framework.

One key recommendation is that risk appetite ought to be articulated, implemented, and reviewed on a continuous basis, with the direct involvement and support of the Board of Directors and senior management. The Risk Appetite Report stated that "Board directors should set the framework for risk appetite and put into place mechanisms to ensure the decision making will be consistently and transparently guided by it."¹⁹ Such involvement is essential, since Boards bear the ultimate responsibility of defining the strategy of the firm and providing oversight of risk management.

Similarly, the Risk Appetite Report stated that "a clearly articulated statement of risk appetite and the use of a well-designed risk appetite framework to underpin decision making are essential to the successful management of risk."²⁰ Risk appetite can provide a consistent framework for understanding risk throughout the organization, and a risk appetite framework provides a context for such traditional risk management tools as risk policies, limits, and management information based on clear risk metrics. The risk appetite framework cannot be a substitute for controls and limits already in place, and neither should it create a whole new set of complex and granular limits. Effectively cascading the risk-appetite framework through the organization and truly integrating it into day-to-day operations is one of the key outstanding challenges raised in the Risk Appetite Report.

Risk appetite was one of the specific areas covered in the IIF and Ernst & Young Survey (2012). Not surprisingly, the survey indicated that developing, implementing and embedding risk appetite was one of the top three areas of focus for Boards and CROs. Many organizations have established risk appetite at the firm level, but cascading it down to the operational level and embedding it in decision making is still a challenge (in fact, this was listed as the top challenge for 75 percent of respondents). Similarly, using the risk appetite framework as a dynamic tool for managing risk was listed as a challenge for 55 percent of respondents.

The survey results and discussions indicate that firms are confronting key practical challenges in implementing a robust risk appetite framework. Three challenges of particular importance are discussed here:

- linking risk appetite to the planning process and being able to demonstrate a functional link between the two,
- effectively cascading risk appetite through the organization, and
- development of risk metrics, including linking risk appetite to risk limits.

2.2 IMPLEMENTATION CHALLENGE – LINKING RISK APPETITE AND PLANNING

Developing and setting the firm's risk appetite should be integrated into strategic and corporate planning at the beginning of the process. Achieving this in practical terms, especially in large and diverse organizations, can be difficult. Integrating the strategic plan and risk appetite, which have historically had different functions and used differing targets and metrics, is proving challenging for many firms.

Link to Strategic Planning

Risk appetite goes far beyond an improved framework for setting risk limits. It provides a means by which risk considerations can be made to permeate all aspects of the business, including strategy and resource allocation, which were previously areas in which formal risk analysis often had little input. This includes assessments of new business opportunities, liquidity, funding, and capital planning.

¹⁷ The SCI report defined risk appetite as "the amount and type of risk that a company is able and willing to accept in pursuit of its business objectives."

¹⁸ Institute of International Finance, *Implementing Robust Risk Appetite Frameworks to Strengthen Financial Institutions*, June 2011. (Risk Appetite Report)

¹⁹ Ibid, 12

²⁰ Ibid. 14

To link risk appetite to planning requires translating the qualitative and quantitative elements of the risk appetite into financial and non-financial targets that can be incorporated into resource-allocation decisions that will impact the business directly on a day-to-day basis. Integrating risk appetite into financial targets and other metrics is another way of communicating the organization's attitude toward, and tolerance for, risk both internally and externally.

Some firms develop their risk appetite based on the strategic plan, whereas others begin by setting the risk appetite as the first step. Different governance frameworks or business models may mean that it makes sense to have a different sequencing of risk appetite setting and strategic planning. What is important is not so much which comes first, but rather that the risk function is involved in the planning process from the onset.

Key to this process is a strong partnership of senior management, including the CEO, the risk function, the strategic planning function and finance. Some firms initially were concerned that including risk in the planning process could complicate existing planning and budgeting processes. However, firms have found that including risk has been well worth the effort. The result has been an alignment of risk and strategic plans, and as firms gain experience with the process they have found that it becomes more efficient over time.

One particularly useful means to link risk appetite and planning is the concept of the firm's "risk posture."²¹ This involves having the business quantify whether more, less, or the same amount of risk will be taken over the next planning period. Framing the discussion in terms of risk posture allows staff to participate in discussions on risk in non-technical language that is widely understood throughout the firm. The planning process is also the time to introduce risk/reward trade-offs. Firms can discuss these in terms of wider corporate strategy and the desired business mix. In fact, the strategic planning function has found that including risk in strategic discussions is more beneficial than originally expected.

Role of the CRO

Planning has traditionally been the purview of the finance function, and many organizations are actively encouraging the CFO and the CRO to work together more closely as recommended in the Risk Appetite Report. One way to strengthen the link between risk appetite and the organization's business strategy is to involve the CRO and risk management in the corporate planning process.

In many firms, it is the CRO's role to ensure that risk appetite and the strategic plan are fully integrated. The IIF and Ernst & Young Survey²² indicates that most CROs have an active role in strategic and planning decisions. With the involvement of the CRO and the increased profile of risk, firms are finding that there is an iterative loop – the risk appetite builds on the high-level strategy, and the strategy is further developed based on the risk appetite.

2.2.1 Example of Practice – Linking Risk Appetite and Planning

One firm uses a Medium Term Planning (MTP) process that usually starts in June prior to the beginning of the annual planning process in the autumn. During the planning process the firm's Management Board reviews actual performance versus plan and current market conditions. This review includes a discussion on strategy and financial targets, as well as an assessment of trends and developments in risk management, the risk appetite framework, and the impact of regulation.

The next step in the process is the Planning Letter, sent out by the CEO to the business units in August or September. This Planning Letter provides high-level guidance for the business unit plans' and normally goes through several iterations before being finalized. The risk function is heavily involved in the drafting of the Planning Letter and is particularly focused on growth restrictions for certain asset classes and countries, limitations on business with counterparties for which no collateral agreements are in place, and investment restrictions. The Planning Letter explicitly states that the plans of individual business units should be in compliance with the firm's risk policies and its various risk appetite statements.

Business units, with the involvement of local risk functions, develop their own MTP on the basis of the Planning Letter. Before submission to the Management Board for approval, corporate risk challenges these plans by giving feedback on, for example, Risk Weighted Asset (RWA) growth in relation to capital targets and risk appetite. This feedback is taken into account in the revised versions of the business units' MTPs. Another check is performed by corporate risk on such

²¹ Institute of International Finance, *Implementing Robust Risk Appetite Frameworks to Strengthen Financial Institutions*, June 2011 (Risk Appetite report), 31.

²² Institute of International Finance and Ernst & Young, *Progress in Financial Services Risk Management: A Survey of Major Financial Institutions*, June 21, 2012. (IIF and E&Y report)

nonfinancial risks as operational, legal, and compliance risks to assess whether appropriate steps have been taken by local business units to control these.

Throughout the process, there is frequent interaction among finance, risk, strategy, and the Boards of local business units. This interaction and coordination is crucial to the success of the MTP process, and challenge is encouraged. In one case, the risk function suggested that aggressive lending growth included in the plan would not be likely to be funded by the commensurate increase in deposits projected, and that alternate funding would need to be proposed if lending targets were to remain intact. This iterative process can involve negotiation between the business and risk; however, the final decision is made by the Board.

Last year business units were provided with a balance sheet optimization tool to support the MTP process. This tool was developed with close cooperation between finance and risk and was designed to raise awareness of the effects of Basel III regulations on the firm. In the model, the optimal balance sheet can be determined given a number of different Basel III constraints RWA, loan-to-deposit ratio, leverage ratio, Liquidity Coverage Ratio (LCR), and Net Stable Funding Ratio (NSFR). The intention was not for the model to mechanically determine the MTP, but rather for it to be used as a supporting tool to assist decision making on the volume targets for the various asset and liability classes.

The increased cooperation between the finance and risk functions has been a tangible byproduct of the MTP process, both improving the planning process and strengthening the link between the firm's risk appetite and strategy.

2.3 IMPLEMENTATION CHALLENGE – CASCADING RISK APPETITE

Linking risk appetite, actual business decisions, and accountability for those decisions is critical to implementing a risk appetite framework. The organization's risk appetite, tolerance and risk limits should be defined in a way that is relevant for the business. Staff in the business units should be able to answer the question – "What does risk appetite mean for me?"

Iterative Process

Once the firm's risk appetite framework has been agreed upon, it needs to be turned into meaningful guidance for the business. Business units typically are responsible for determining their local risk appetite, often with the assistance of the risk function. The Risk Appetite Report stressed that for the risk appetite framework to be effective, it should be pervasive throughout the firm, and staff should understand not only the organization's approach to risk, but also what this means for them individually. The heads of business units have the primary responsibility for cascading risk appetite as well as for articulating the benefits of using the risk framework to their staff. It is important for the CRO, senior management, and especially the CEO to visibly support the risk appetite framework, explaining and reinforcing the need for it to be fully incorporated into the day-to-day operations of the organization. However, embedding risk appetite cannot be the primary responsibility of the risk function or the CRO, but should be driven by the business.

In practice, setting the risk appetite framework is an iterative process. Individual businesses check to ensure that their risk appetite is consistent with the overall framework, and at the same time a check is done to verify that the sum of the various business-line frameworks does not exceed the overall risk appetite. Although the analysis of the individual business risk appetite frameworks may fall to the risk function, it is the Board and senior management who make any decision about changing the individual frameworks or amending the overall risk appetite.

This process can be time-consuming and requires systems able to integrate data from different businesses and jurisdictions, which may be in different formats. The challenge is to take multiple inputs and convert them into a common format that allows for aggregation and comparison, which can then be translated into a document staff can understand and use. In the end, the firm should be able to produce a risk appetite framework that provides high-level guidance for the Board and senior management to be used in the planning process and can serve as a reference for staff in their day-to-day risk decisions. Widely disseminating the risk appetite framework through the organization is a way to increase internal transparency about risk and help staff understand their role in risk management. However, dissemination needs to be carefully considered, as the framework needs to be meaningful and comprehensible to all.

The iterative process of developing the risk appetite framework may be used to the firm's advantage, making it a dynamic tool for shaping the organization's risk profile. Implementation of the risk appetite framework is still a relatively new process for many firms and whether risk appetite can be used as a dynamic tool depends to

a large extent upon whether the framework has been institutionalized and embedded within the firm. Fostering an ongoing dialogue about risk appetite that involves senior management, the business and the risk function facilitates a positive evolution of the framework and can play a role in developing a challenge culture.

2.4 IMPLEMENTATION CHALLENGE – DEVELOPING RISK METRICS

Organizations need to develop metrics to monitor its risk profile against the stated risk appetite. There should be a consistency of metrics used throughout the firm, yet they must be meaningful and measurable in diverse business units. One issue is the sheer number of risk metrics used to assess risk appetite and the problem of identifying which metrics to use to hold an individual accountable. In many cases, quantitative limits will not be sufficient if the metrics used do not cover all risks, especially such non-financial risks as reputational or legal risk.

2.3.1 Example of Practice – Choice Modelling

One firm uses “choice modeling” (a technique borrowed from marketing) to help develop its risk appetite. Choice modeling is a technique that teases out the factors people use in making decisions. The technique pits difficult choices against each other (e.g., questions about price and convenience, which identify the factors driving a decision about where to shop). People are forced to make trade-offs and prioritize choices. This is relevant, since risk appetite is implicitly an expression of the organization’s preferences when it is forced to make difficult business decisions.

The exercise is conducted using an automated blind voting system. This is considered useful because it ensures that the views of all participants are taken into account and minimizes bias caused by strong personalities (e.g., the CEO or Chair) dominating the outcome, as can sometimes happen in group discussions.

Choice modeling has been used at the Board level, at the Executive Committee level, and at the leadership team level for each of the major operating businesses. At the Board level, the exercise culminates in a Risk Appetite Statement (RAS), a high-level, four-page document that outlines principles and guidelines for the businesses to follow. The RAS also incorporates, by reference, all operating limits previously approved by the Board.

Operational business unit RAS documents, which are also approved by the Board and collectively form part of the overall group RAS, are much more extensive and more directly linked to business parameters and drivers. These also are explicitly linked to the strategic and capital plans of specific business units. RAS documents are developed concurrently with strategic and capital plans, where the inherent tension between capital capacity, strategic aspirations, and risk appetite is transparently played out over the three to four month planning cycle. The approach is now evolving to the point where all three components are updated on a regular basis as the financial year progresses.

By using choice modeling at multiple organizational levels, useful differences in the preferences between the Board and line management can be revealed. For example, when confronted with a scenario involving serious asbestos problems in a major building, the Board was extremely conservative in its preferred organizational response, whereas the premises management team was much more sanguine, confident in its ability to manage the situation in a cost effective manner without an urgent response. This difference in perspectives gave rise to a robust discussion, with the Board’s preference winning the day. Usefully, this has now given the firm’s risk management team a clear area of focus for ongoing governance and monitoring, to ensure line management abides by the Board’s expressed preference.

RAS documents are usually drafted by a CRO, presented for discussion, and massaged into a final form approved by the Board. Use of choice modeling was found to better draw out the combined risk preferences of the Board, and to do so with less pre-positioning bias. It also helped directors better understand their own collective thinking.

Choice modeling may not solve all the problems firms face in cascading risk appetite. It is however, an approach that can highlight discrepancies in the practical understanding of risk appetite within the firm. Asking the Board and the business units to prioritize risk choices is a reflection of the decisions that must be made at all levels of the firm in an environment of limited financial and other resources.

High-Level Outcomes

The IIF report listed a number of qualitative and quantitative outcomes firms have used to define metrics under risk appetite statements. Qualitative outcomes included target credit ratings, regulatory requirements, and maintaining a well-diversified funding structure, among others. Quantitative outcomes included target Tier 1 ratios, return on equity, earnings volatility, risk weighted asset limits, liquidity ratios, and industry concentration limits.

Metrics

Although risk appetite statements should include a number of outcomes, a recent trend is for organizations to refine and reduce the number of qualitative and quantitative metrics used for risk appetite purposes. Some firms have found that too many metrics can make it difficult to hold the business accountable. Getting the number of metrics right is a difficult balance, as too few may not be meaningful, whereas too many can result in a loss of focus. The rationale for a limited number of high-level metrics is that it is unlikely that all staff would be able to answer "What does risk appetite mean for me?", if too many metrics are used.

Going from a high-level risk appetite statement or framework, to metrics that are understood and used by line management can be challenging. At this stage, the objective should be to move beyond generic outcomes (e.g., a desired rating for the firm) to specific business decisions and targets that are reflected in the firms' financial and non-financial objectives. In defining core metrics, it may be helpful to articulate an outcome—for example, loss—which can be applied universally.

It is important to point out that not everything can be aggregated, even for the same type of risk. For example, credit losses, in the wholesale banking business are different from those in wealth management. The starting point is that when a metric makes sense for the business, it should be defined and included – even if it is not additive to the group-level metrics.

Core, Supporting, and Monitoring Metrics

One approach to cascading risk appetite is to divide metrics into three categories. Core metrics are those to be applied across all businesses and risks. These articulate the risk appetite and provide a common language across risks and businesses. *Supporting metrics* are those applicable to a specific risk type across all business units. These support the articulation of risk appetite and may be quantitative or qualitative. *Monitoring metrics* are ones applicable within the specific risk type and within the business unit. These metrics are aligned to the risk appetite measures but are not part of the risk appetite statement; they are used by the

business in day-to-day risk management.

Some examples of high-level metrics used by firms are:

- credit rating
- concentration limits (e.g., the top exposures as a percentage of Tier 1 capital)
- regulatory capital adequacy
- economic capital adequacy
- VaR
- earnings
- solvency
- leverage ratio
- stability of earnings
- liquidity and funding risk requirements
- exposure to stress events

Regular Reporting of the Risk Profile

Reporting of risk profile relative to the firm's risk appetite should be in place to drive ongoing discussions and analysis of the firm's approach to risk. These discussions should include senior management, the business, and the risk function. In addition to highlighting potential breaches of risk limits, escalation procedures to alert line management before risk tolerances are exceeded are required to truly link risk appetite to risk management. To reinforce this link at the highest level, the role of the Board in authorizing temporary breaches of risk appetite, or in changes to the risk appetite outside of the planning process, should be clearly articulated. If the firm's risk appetite is exceeded, the Board should be informed and management should present a plan to deal with the breach.

Linking Risk Appetite to Risk Limits

Linking risk appetite to risk limits can be one of the most challenging aspects of cascading risk appetite. Many firms try to create multiple links to limits, which can be complex and impractical. It is important to have a clear and structured set of limits, and it may be helpful to make a distinction between a limit that can be easily controlled, such as lending volumes, and a metric like average loan-to-value (LTV), which is more difficult to control. It should be noted that it is essential to have the facility to run stress tests quickly to provide sufficient granularity to determine the segments of the portfolio where, for example, losses are likely to arise.

Linking risk appetite to risk limits can be described as part art and part science. Although some firms align risk appetite to risk limits, not all firms are yet fully able to make the link. One approach is to incorporate trigger levels

for risk appetite tolerance, with clearly defined escalation procedures and action plans. The business should drive the process of linking risk appetite to its risk limits; however, it should be recognized that this may not be a straightforward "one-size-fits-all" exercise. Nor should immediate results be expected, as it can take time to get the alignment right. Taking the time needed is preferable to rushing the outcome and producing results that do not assist the Board and senior management in making informed decisions.

Breaches of Risk Appetite

There are a number of circumstances in which a firm's risk appetite may be breached, and not all are the result of noncompliance or are cause for disciplinary action as described in the discussion of risk-based compensation earlier.

When the risk appetite set by the Board is cascaded through the firm and individual businesses determine their risk appetite, the aggregation of the individual risk limits may be above that defined in the overall risk appetite. The Risk Appetite report²³ described an iterative process starting with a concept of risk appetite -> business planning -> aggregation -> checking back with the risk appetite framework and adjusting as necessary.

In other cases, there may be inadvertent breaches of the risk appetite, temporary or otherwise. These types of breaches are normally dealt with on a case-by-case basis and escalated based on severity, duration of the breach, and other factors a firm considers relevant for the specific risk.

2.4.1 Example of Practice – Developing Metrics

At one firm most *first-level* (core) metrics are those that involve financial risk, such as the ratings, capital and liquidity targets listed earlier. Its *second-level* metrics are stressed versions of these core metrics; for example, in an adverse 1-in-10-year scenario, Tier 1 capital should remain above a certain threshold. These second-level metrics are in effect the firm's risk tolerance, and it is when these are breached that the Board is informed. Any report to the Board includes information about what factor is driving the breach and, for example, how much Tier 1 capital could drop, and for how long, before risk appetite was exceeded.

If there is a problem with a breach of the second-level metrics, or risk tolerance, the issue is escalated to the Board level. In such an instance, the CRO prepares the risk mitigation or action plan to remedy any breach of the firm's risk tolerance. Metrics may be monitored using stress scenarios, and one approach is to define trigger points for automatic escalation of breaches at three levels: normal, stressed and crisis.

The Board is formally involved in approving the concepts used in risk appetite as well as the first-level and second-level metrics, which are not changed much over time. Senior management goes into more detail on the first-level and second-level metrics, and sets the *third-level* metrics. An example of a third-level metric is exposure at default for certain asset classes. These third-level metrics have to be in line with the risk tolerance determined as second-level metrics and are reported to senior management and Asset Liability Committee (ALCO) monthly.

Linking these metrics to risk limits is the most difficult step. The objective, which is largely being met, is for the top-down allocation of risk appetite to drive the process. The firm takes advantage of a number of opportunities to better align cascaded risk appetite with risk management limits, and these occur:

- when the risk appetite framework is reviewed,
- during medium-term (1 – 3 year) planning discussions,
- at the time new initiatives are being approved, and
- if existing limits are breached.

In any case, all limits are reviewed annually, and this provides another opportunity to fine tune allocations and cascade risk appetite. Any changes made would be to the firm's risk profile (risk limits), not to its risk tolerance (second-level metrics).

²³ Risk Appetite report (2011), 30.

However, the Board may not need to be informed every time there is a short-term breach of a risk limit. If, for example, there is a breach of a VaR limit for one day this may only be reported to the Board at quarter end. The question for management to ask is not only if the breach is material, but also if action must be taken to remedy the problem.

Finally, there are deliberate breaches that may be the result of a strategic decision. These are not the result of a disregard for risk or an attempt to beat the system. An example of a deliberate breach for strategic reasons is, in the case of a firm using Tier 1 capital as a risk target - if an acquisition would cause the Tier 1 ratio to fall below target. In this case, management would inform the Board of how long the ratio would be below target and actions to be taken to rectify the situation.

Whatever the cause of a breach of risk appetite, firms should have in place processes to detect and monitor breaches as well as escalation procedures, and they should have the ability to quickly implement action plans to correct the situation. The capability to put into place a proportionate and targeted action plan should be the ultimate objective.

SECTION 3. ORGANIZATIONAL STRUCTURES – ROLE OF THE BOARD AND BOARD RISK COMMITTEES

3.1 OVERVIEW

Increased Board engagement in risk management is commonly agreed to be essential to strengthening risk governance. It is important that the Board's risk committees have a strong and central role and that their members have the expertise and experience to make rigorous and informed judgments on risk, including the incorporation of risk considerations into the overall strategy of the organization. The IIF²⁴ has emphasized that the key Board-level oversight responsibilities include reviewing strategy and approving and overseeing the firm's risk appetite framework.

Recommendations on risk governance generally include increasing Board oversight of risk and significantly increasing the amount of time allocated during Board sessions to the discussions of risk management issues. Both the FSB and the Basel Committee on Banking Supervision (BCBS) have focused on the importance of Boards involvement with risk management. The Basel Committee's *Principles for Enhancing Corporate Governance* raises the issue of Board oversight and outlines three principles for Board practices:

1. The Board has overall responsibility for the bank, including approving and overseeing the implementation of the bank's strategic objectives, risk strategy, corporate governance, and corporate values. The Board is also responsible for providing oversight of senior management.
2. Board members should be and remain qualified, including through training, for their positions. They should have a clear understanding of their role in corporate governance and be able to exercise sound and objective judgment about the affairs of the bank.
3. The Board should define appropriate governance practices for its own work and have in place the means to ensure that such practices are followed and periodically reviewed for ongoing improvement.²⁵

Most organizations have already embarked on programs to strengthen the risk governance role of their Boards, with Board involvement and focus on risk increasing significantly since the financial crisis. This requires an increase in both the amount of time spent on risk issues and greater risk expertise on the Board. At the Board level, enough directors with the right expertise are needed, and organizations are changing the composition of their Board to strengthen risk governance.

Dedicated risk committees have been established by many firms. This is an important step for firms where risk was not an explicit element of the Board's agenda. While the establishment of risk committees is intrinsically a positive step, firms also should consider that different kinds of risks may be best suited to the expertise of different committees.²⁶ Having various committees play complementary roles in risk oversight (for example, the credit risk committee or the audit committee), and sharing their findings and insights with each other and the entire Board can help set the tone that risk oversight is the concern of the full Board. Regardless of the committee structure chosen, as noted in the Walker report²⁷, it is important that the whole Board is ultimately responsible and accountable for risk governance.

It is worth noting that governance committee structure, both at the Board level and at the executive management level, is an area that shows the widest variation across different financial institutions. In many cases, this is due to varying regulatory requirements in different jurisdictions, which in some cases mandate specific committees and membership structures and obligations. It is also due, appropriately, to significant differences in the size, complexity, and cultures of firms – smaller, less-complex financial institutions do not need the same governance processes that a very large international organization requires. Another key factor is differences in legal regimes, in which directors of subsidiary Boards in some countries face varying degrees of personal liability, and therefore have a much stronger interest in risk governance at the local level.

²⁴ IIF, *Final Report of the IIF Committee on Market Best Practices: Principles of Conduct and Best Practice Recommendations* (CMBP report), July 2008.

²⁵ Basel Committee on Banking Supervision, *Principles for Enhancing Corporate Governance*, October 2010, 7-11.

²⁶ See Wachtell, Lipton, Rosen, and Katz, *Risk Management and the Board of Directors*, December 2010.

²⁷ Walker, David, *A Review of Corporate Governance in UK Banks and other Financial Industry Entities – Final Recommendations*, November 2009.

Notwithstanding this wide degree of variability across organizations, there are key principles that are consistently in place across all well-run companies:

- clarity of roles and responsibilities among the different committees, to ensure that all key risk areas are covered with minimal duplication and second guessing;
- clear and documented communication of decisions made by committees both upward to more senior committees and downwards to the business units; and
- a strong focus on ensuring that governance committees at all levels have members with the skills and capacity required to carry out their responsibilities effectively.

The IIF and Ernst & Young Survey²⁸ indicates that Boards are now more actively engaged and involved in risk policy setting and governance. Many firms report changing the composition of their Board to upgrade experience and skill on risk (37 percent of respondents), banking experience (35 percent of respondents) and the regulatory expertise of Board members (13 percent of respondents). An overwhelming majority of respondents (87 percent) reported stand-alone, Board-level risk committees. More than three quarters of those banks with risk committees reported some overlap in membership between their audit and risk committees.

As firms delve into the implementation of significant changes in their governance structures and procedures, a number of challenges arise. These include achieving the right mix of Board members, making the process of interaction between senior management and the Board more effective, and achieving the right balance on the degree and content of intervention of the Board on risk matters. More specifically, some of the key challenges faced by firms strengthening risk governance and organizational structures are:

- building strong risk governance committees,
- managing the interaction of various Board and executive risk committees,
- achieving comprehensiveness while maintaining comprehensibility in risk reporting to the Board,
- providing the Board with meaningful stress test results and associated risk analysis to facilitate strategic decision making, and
- conducting Board self-evaluations to assess how the Board fulfills its risk responsibilities.

3.2 IMPLEMENTATION CHALLENGE - STRENGTHENING BOARD RISK COMMITTEES

Increased focus on risk at the Board level can present problems for firms trying to staff the risk committee quickly with directors who have the requisite risk expertise. It can sometimes take time to find Board candidates who combine solid and relevant risk experience with the stature and judgment required to confidently challenge management on risk.

Two-Tier Board

Two-tier Boards typically include a Supervisory Board composed of stakeholders and independent directors and a Management Board. Members of the Supervisory Board, who represent shareholders and other stakeholders, are directors who would generally be considered non-executive and/or independent directors in a single-tier Board structure. Members of the senior management team, including the CEO, CFO, CIO, and CRO usually make up the Management Board in a two-tier framework, which may alternatively be called the Executive Committee in a single-tier Board structure.

Whether under a single or two-tier Board structure, proper boundaries should be drawn between the executive role of management and the Board's non-executive role.

Increasingly, dedicated Supervisory Board risk committees are being established, with terms of reference, including interactions with the Board and other Board committees, clearly spelled out. The risk committee includes directors with an understanding of risk management issues and auditing. Both the CFO and CRO typically attend meetings, and the CRO's role as a participant on the risk committee of the Supervisory Board is to ensure that directors on the committee are fully aware of the firm's risk position, through regular reports from the business on risk appetite and risk profile. The Supervisory Board risk committee may delegate some risk management responsibilities, for example, policies, processes, and controls, to the Management Board risk committee, where the CRO is typically a member and usually coordinates meeting agendas.

²⁸ IIF and Ernst & Young survey (2012).

Role and Responsibilities of the Board Risk Committees

Whether an organization has one Board-level risk committee or several specialized committees, the terms of reference of all Board committees should clearly set out:

- their responsibilities for risk, including risk oversight,
- their relationship – including regular formal interactions – with the other Board committees and relevant management committees, and
- their relationship with the wider Board.

Building a strong risk committee with the requisite expertise and qualifications to guide corporate governance at the Board level has been a priority for many organizations since the recent financial crisis. The risk committee in the aggregate should have members with an understanding of risk; combining members who can provide wide business or financial experience, so the committee collectively will be able to form judgments on the organization's risk taking and risk management.

Although the process of strengthening the risk committee is a long-term commitment, the results can be extremely valuable. Firms have found that informed and educated members of the risk committee add significant value to the governance and decision-making processes.

In many cases, some Board members will have the required skills; in other cases, there is a need to externally recruit new members to the Board. Unfortunately, candidates with the right experience are not always available immediately. Once recruited, the process of educating new Board members on the organization's corporate and risk culture is crucial. As in filling positions on all Board committees, the role of the Nominations and Appointments Committee in finding the right candidate should not be underestimated.

Members of a Board Risk Committee are typically drawn from the main Board, and firms would not generally appoint directors to the Board risk committee who are not on the Board. However, some Board risk committees may periodically engage independent advisers to provide a fresh perspective, and to possibly identify any gaps in coverage.

3.2.1 Example of Practice – Board Risk Committee Composition

One firm took the opportunity to alter the composition of its Board risk committee after a merger. The objective was to include Board members with a deep understanding of risk management and bring expert judgment on both existing and emerging risks to the committee. The risk committee is composed of a majority of independent directors who have extensive banking and financial market experience. In particular, the firm believed it was important to include people with financial industry experience in its home market as well as internationally.

This firm appointed a former central bank Governor to the risk committee to bring a non-business perspective to risk discussions. To ensure that a thorough understanding of the bank's operations is given prominence in deliberations, the CEO and the Head of the Wholesale Bank are also members of the committee. The inclusion of these highly experienced bankers helps to link high-level, strategic discussions of risk with the day-to-day operations of the firm. In summary, the reconstituted risk committee has made a major contribution to risk discussions by adding a fresh perspective as well as by making concrete suggestions on risk management practices.

Another firm has taken a different approach. This firm has sought a balanced mix of Board members, with some possessing senior management experience outside the financial industry. In particular, one Board member has experience in the retail industry and is able to credibly challenge fellow directors on marketing issues. The firm believes that for a bank with a large retail client base, this can be a real advantage. Another Board member has a trading background, and the bank has found that this director's experience and judgment adds a valuable perspective to Board decisions. The point that this bank would make is that the risk experience needed on the Board does not have to reside in one person, and that the best mixture of experience and people is in part determined by the firm's business model.

One important factor in Board composition is the stature of members and their ability to challenge senior management. An over-emphasis on risk management experience may not result in the diversity of expertise needed for the Board to challenge senior management or the Chair if needed. Another issue that should not be overlooked is the increasing time demands on Board members, which result in the need to consider how to best leverage Board expertise on risk.

It is essential that Board members have risk knowledge, but some firms believe that this knowledge may not necessarily be gained only through formal risk training or risk management experience. Appointing Board members to the risk committee based only on their risk management background may not result in the kind of constructive challenge culture needed for a productive dialogue on risk. It is Board members' ability to think strategically about risk, their judgment, and the broader perspective they bring to deliberations that can be the most valuable in promoting a challenging yet constructive dialogue on risk.

As previously stated, the IIF notes that there is a great deal of variability in the structure of Boards and Board risk committees. These differences may be driven by legal requirements, regulatory requirements, or both, or by historic practice, as in the two-tier Board structure described below. However, the guiding principle in assigning responsibility for risk at the Board level should be to use a structure appropriate for the organization's nature, scale and complexity.

3.3 IMPLEMENTATION CHALLENGE - INTERACTION OF BOARD RISK COMMITTEES

Some organizations do not have a single risk committee as such, but instead have various other committees that have within their remit some aspects of the risk oversight function. With multiple committees dealing with risk, it is important to consider the danger that risks might fall between the cracks, or that risks are dealt with in silos and their interaction is not properly assessed and considered.

Responsibility of the Board

Ensuring that all risks are covered and that the interaction between various risks as well as concentration risk is dealt with is a basic responsibility of the Board. Reporting lines of various committees responsible for risk should be structured in a way that strengthens risk management, avoiding overlaps and, especially, underlaps. These reporting lines should take into account cultural and organizational differences while ensuring that risk is looked at holistically and remains the ultimate responsibility of the whole Board.

There are many possible structures that can work in principle; although it is essential that all committees and subcommittees have clear mandates and terms of reference that set out, inter alia, how their roles interact with those of others. The various committees dealing with risk should all work toward a shared set of consistent and commonly understood objectives which derived directly from the risk appetite. Communication among committees is essential, and cross-membership on various risk committees is one

possible way of achieving this.

Delineation of Responsibility

One of the issues faced by organizations in strengthening risk governance is delineating responsibilities among the Board, the Board risk committees, and senior management. Some firms have adopted cross-membership on Board committees in an attempt to ensure that all risks are covered; for example, the Chairs of the risk and audit committees may have a seat on each other's committee.

One argument for separate risk and audit committees is that combining both in one committee may reduce the ability of the audit staff to independently challenge the risk function. While the IIF²⁹ suggested firms consider whether to have separate audit and risk committees, it has acknowledged that the characteristics of the individual firm should be considered. Whichever structure is chosen, changes in the role and reporting of internal auditing and compliance to strengthen risk governance should be considered and implemented, if required.

Involving multiple Board and other non-Board-level committees in risk creates a danger of dispersion of responsibility with no ultimate accountability, or the opposite, the development of a silo mentality without adequate coordination or aggregation of risk. Some firms have found that involvement of the Board Secretary is useful in coordinating agendas and mitigating the possible confusion that could result from cross-membership on Board committees, whereas other firms look to the Chair to take responsibility for coordination. Typically, a Group CRO also plays a key role in this area.

²⁹ IIF, *Final Report of the IIF Committee on Market Best Practices: Principles of Conduct and Best Practice Recommendations*, July 2008 (CMBP report).

3.3.1 Example of Practice – The Interaction between Group and Local Boards

The relationships between group Boards and local Boards, in which local entities are required to make independent decisions or have their own Board risk committees needs to be reconciled. In many firms, cross representation on local and group Boards supports and ensures the alignment of overall objectives. Banks increasingly report constraints imposed by host supervisors on cross-representation or on local subsidiaries' Board procedures or decisions (e.g., requiring an exclusively local view of liquidity-risk management that de-emphasizes group resources or objectives), which can potentially affect the alignment of overall objectives across a group. Local resolution plans are another example of the constraints to which Boards may be required to manage.

Notwithstanding this, there are examples of the opposite approach. For example, a conglomerate was recently restructured under a regulator approved holding company structure, in which one common set of directors serves as the Board both at the holding-company level and at each of the major regulated subsidiary businesses. The key driver for this structure was a clear desire by the Supervisory Board to ensure consistency of the enterprise risk management framework across the group, and to facilitate more constructive conversations about relative risk-adjusted performance by different businesses in their use of capital.

An annual process of assessing the extent to which the risk dimensions of local plans fit within broader risk appetite objectives is required in many groups, and any material issues arising from the reconciliation of the two should be explained to the main Board. The business should be expected to explain how its business and financial plans have taken account of, and fit into, enterprise-wide risk objectives, and to explain any local legal or regulatory constraints that they have had to take into account, such as requirements to maintain local pools of liquidity, constraints on sharing data with group risk functions, or requirements of local recovery and resolution plans that may affect risk objectives or risk management.

Risk considerations should figure prominently in the business and financial plans of local business units, with central risk management involvement in local risk planning and decisions. Discharging legal requirements for the independence of local Boards and explaining how this can be done, while maintaining alignment with group objectives and adherence to group targets, should figure prominently on the agendas of local Boards. Any instances in which local requirements require deviation from group objectives or targets should be explained carefully and escalated.

3.4 IMPLEMENTATION CHALLENGE – RISK REPORTING TO THE BOARD

It is important that the Board be given information that allows it to understand and appreciate risk issues, challenge management on risk decisions, and have a plain language conversation about risk at the Board level. The biggest risk reporting challenge for many firms is balancing comprehensiveness and clarity to enable the Board to focus on decision making.

Managing The Volume of Information

Board and Board risk committee members can often be presented with a great deal of data, information and reports on risk. Every effort should be made to avoid producing raw data and to concentrate on producing information that is:

- timely,
- concise,
- comprehensive, and
- actionable.

The ultimate objective is to provide risk reporting that enables the Board to reach informed decisions on risk issues. The CRO, working with the CEO and senior management, should ensure that risk reports to the Board contain meaningful information on the firm's overall risks, risk concentrations, emerging risks, and any changes or trends in key risks. The business should be responsible for providing analysis of information reported to the Board and Board risk committees; however, the CRO is in a position to augment this analysis by making recommendations based on a broad understanding of the firm's total risk profile.

Firms struggle to avoid providing excessive volumes of information with the attendant problems of interpretation, and the risk that important information is buried. However, aggregating reporting to the point of only looking at a summary of different types of risk on a red, amber, and green "dashboard," while apparently efficient, may result in a loss of detail that can limit discussion at the Board level and may mean that significant risk issues are not brought to the Board.

Role of the Business

The CRO plays a vital role in providing the interpretation and recommendations needed for the Board to make decisions based on the information reported. It is, however, the business that should be the first to call out risk issues at the Board level. The business, along with senior management, also should have the primary responsibility for developing recommendations and action plans to control, mitigate, hedge, or eliminate risks brought to the attention of the Board. These conversations at the Board level should not simply include management, but also should be actively led by the business.

Reporting on Risk Appetite

One of the key reports the Board should be looking at is the monitoring of the organization's risk profile against risk appetite. Some firms run risk aggregation models to determine if actual risk profiles are in line with high-level risk appetite statements. Several risk metrics can be calculated at the firm level to verify alignment with risk appetite. These include earnings-at-risk, revaluation reserves-at-risk, risk-weighted assets-at-risk, and economic capital on a stressed basis.

3.4.1 Example of Practice – Risk Reporting

At a typical meeting of the risk committee of the Supervisory Board of one firm, there are a number of regular risk items on the agenda, as well as some topics of current interest. The meeting addresses risk from the perspective of historically observed volatilities and data and considers forward-looking items. Some of the regular agenda items for the risk committee of the Supervisory Board are a review of the risk appetite framework and presentation of a financial risk management report, as well as a discussion of a report evaluating non-financial risks. All material for the meetings is prepared by the office of the CRO.

As noted, one of the regular agenda items is the risk appetite framework, which sets out the bank's main risk objectives and is updated on a periodic basis. Changes to the framework may be proposed to better reflect new regulatory guidance, or when adjustments in the firm's strategy require an update. This review provides the risk committee with the opportunity to challenge management on risk decisions.

The financial risk management report provides an overview of the risk appetite framework. Financial risk-related topics like solvency and liquidity positions, and risk concentrations are continuously monitored. Financial risk metrics include reports on how earnings and solvency are affected in a 1-in-10 year scenario. This report enables the risk committee to assess how the bank is currently positioned from a financial risk perspective.

A similar report is presented to evaluate non-financial risks. This report contains a table showing business lines on one axis; and on the other axis are ten risk categories that encompass IT risk, process risk, business continuity, compliance, fraud, etc.

During the meeting, an assessment is made on which risk categories, in which business units, require attention and these are then prioritized.

The firm's business recovery plan is not a fixed item on the agenda; instead, the risk committee monitors the development of high-impact "regulatory" projects. As a lesson learned from the global financial crisis, the firm has set up an inclusive recovery planning process to strengthen the bank's readiness to tackle financial crises using its own resources. In the progress report on recovery planning, an update is provided on how the bank prepares itself to be constantly vigilant with regard to developments that may indicate the emergence of a financial crisis.

Since 2008 a number of topics have been given extra attention by the Board. Current issues, such as the global financial crisis, liquidity, or the European sovereign debt crisis, are discussed by the risk committee. General macro-implications are discussed at the Board level, and specific potential consequences for the firm are also examined.

Forward-looking risk discussions include a number of topics that could develop into potential risks in the future. These topics generally reflect what is being observed in the markets and focus on those items that could negatively influence the firm's portfolio and financial performance. One of the lessons learned from the crisis was that only evaluating current risks is not sufficient – potential emerging risks deserve equal attention, as they may impact current decisions, enabling the firm to better position itself for the future.

Any metrics used should incorporate the impact of different risk types; for example, earnings-at-risk should include credit risk cost and impairments, impact of interest margin, equity impairment, and the impact of operational risk. One firm emphasizes that what is most important is the correlation among the different risk types, as the quality of the outcome is highly dependent on the accuracy of the correlations. This firm believes that if there is any uncertainty about the correlation, it should be set conservatively.

Key and Emerging Risks

An important aspect of risk reporting to the Board is the coverage of key risks and emerging risks and highlighting changes or trends. The Risk Appetite Report recommends periodic reviews to discuss what is new or growing rapidly, what is changing, what's driving those changes, and what the emerging risks are. The topics, or content, covered under key or emerging risks depend upon each organization's business model; however, most organizations believe it is important to use the Board as a forum to focus on strategic and emerging risks.

One firm's approach to key and emerging strategic risks is to annually review every business unit through the lens of the acquisitions team asking the question, "Would we buy this business?" By looking at expenditures, the profit-and-loss statement, and balance sheet risk, as well as benchmark market data, the business unit is compared to similar businesses at other firms. This firm finds this exercise very useful in highlighting and explaining strategic risk to the Board, and also uses it as a way to promote a challenge culture within the organization.

3.5 IMPLEMENTATION CHALLENGE – USE OF STRESS TESTS AND OTHER KEY RISK METRICS BY THE BOARD

Stress testing is used to determine the impact that severe but plausible stresses would have on the firm's balance sheet and financial health. Many firms are still trying to ensure that stress tests presented to Boards facilitate strategic decision making, while simultaneously improving data aggregation and other inputs.

Use of Stress Tests and Risk Metrics

Stress tests and other key risk metrics provide the Board and senior management with a basis on which to satisfy themselves that the firm's controls and financial resources are adequate in the face of stress scenarios. Stress testing and other risk metrics should have a meaningful impact on business decisions, and provide the Board and senior management with the means to implement changes to

the risk profile of the organization. Board-level discussions about risk metrics and stress testing should not ultimately be about technical points, but rather about much more fundamental strategic and risk issues. It is important that Boards are able and willing to take action on the basis of stress tests and risk metrics.

Many firms are going further with their stress testing programs than simply complying with regulatory requirements. For example, they are electing to stress test more frequently, look at a wider range of scenarios than required by the regulator, or undertake firm-specific or micro-stress tests to supplement the macro ones sometimes required by regulators. There is no one approach taken by all firms, as different business models may require different approaches.

Firm's stress tests should be based largely on "well-defined and specific scenarios relevant to the firm."³⁰ This is where many firms are finding that forward-looking scenarios that incorporate risks specific to the organization can be actively used by the Board and senior management in decision making.

Avoid "Silver Bullet" Solutions

It is important that Boards and senior management avoid viewing stress tests as a "silver bullet" solution. In assessing stress tests, Boards and senior management should be cognizant of the risk of model error and the uncertainties associated with models, valuations, and concentration risks. Many assumptions are used in developing stress tests, in addition to the uncertainties associated with the aggregation of risk. One possible approach to improving the quality and utility of stress test results is to set up a data center of excellence to consolidate stress testing for the firm. In this way, the various stress tests undertaken by the firm for internal purposes, as well as those required by regulators, could be better aligned and presented in a format that facilitates decision making.

The IIF and Ernst & Young Survey points out heightened attention to strengthening stress testing strategies, systems, and procedures. Boards and senior management are using scenario planning to consider the various market factors and macro-economics events that could affect the firm. Respondents used stress testing in areas such as capital planning, acquisitions, and new products, in addition to their use in risk appetite development and management. Organizations cited extracting and aggregating data and inadequate systems as the top challenges to effective stress testing. Although many firms are making progress, there are no quick fixes, and improving stress testing is an ongoing process.

³⁰ CMBP report, 48

3.5.1 Example of Practice – Stress Testing

Using forward-looking scenarios can be an important tool in Board decision making. Hypothetical forward-looking scenarios can be helpful, for example, in considering emerging risks and determining longer term strategy. One firm focuses on the severity of macro-economic scenarios in its stress testing and translates the results into impact on earnings and capital. In presenting results to the Board, the firm has found that a visual representation of earnings volatility can be useful in illustrating the impact of forward-looking scenarios.

The limitations and pitfalls of forward-looking scenarios also should be considered, as scenarios rarely unfold exactly as anticipated during their development. For this reason, it is important to inform the Board of how the world has evolved relative to the assumptions used in the stress tests. Incorporating criteria for taking action and accountability into stress test results reported to the Board also is highly important. Many assumptions are used in translating economic events into impact on the P&L or on risk-weighted assets, and value lies in analyzing how the scenario would unfold and what degree of severity would harm the firm, rather than focusing on probability.

Firms have found that it is their use in decision making, rather than the statistical accuracy of forward-looking scenarios, that can be of real importance to the Board. It is this discussion, triggered by whether losses should be accepted, mitigated, or hedged, that is the most valuable, rather than the specific details of the test results. Such discussions should be linked to the firm's strategy, risk appetite, and risk-limit setting. An important role of the Board is to determine how flexible the firm could be in responding to a crisis.

In short, at the Board level, it is the discussion generated from the actions that would be taken in the event of a crisis that is the true benefit of the stress-testing process.

3.6 IMPLEMENTATION CHALLENGE – BOARD SELF-EVALUATION

With increased regulatory pressure for Boards to take more responsibility for risk governance, it is important that Board members are confident that they are meeting stakeholder expectations, and self-evaluations are one way of doing this. The challenge lies in using self-evaluations as a diagnostic tool to make improvements in Board risk governance practices. Teasing out the root cause of any problems or inefficiencies uncovered as a result of a self-evaluation requires an objective analysis of the results and a willingness by Board members to critically examine their interaction with the firm's management and with each other.

The Self-Evaluation Process

Prior to any Board self-evaluation, it may be useful to review the Board's internal guidelines and committee charters. For many firms, a comprehensive and coordinated Board committee agenda matrix is a prerequisite to producing a meaningful and actionable self-evaluation.

Evaluations should include a focused set of questions and a simple scoring system. Of paramount importance is evaluating Board reporting and demonstrating that Board and committee members receive information that facilitates decision making. Unsurprisingly, firms that have completed Board evaluations have found that continuous training is required to enable the Board to adequately fulfill its risk responsibilities.

Actionable Results

To contribute to improved Board risk oversight, any self-evaluation should be designed to produce actionable results. It is this last element that can be problematic. Teasing out substantive recommendations for change from Board responses to qualitative and subjective questions can involve a good deal of interpretation and may not be as precise and specific as desired.

The fundamental question to be asked is, "Has the Board made a difference?" Is it possible to point to instances in which outcomes would have been materially different had the Board not intervened in certain ways? One factor to consider in assessing the ability of the Board to make a difference is to gauge member willingness and ability to challenge the Chair. Some firms believe that a certain amount of constructive tension can be helpful in improving Board decision making. On the other hand, the CEO or Chair must be respected by the directors for there to be a productive dialogue.

Self-Evaluation Questions

Although there is no standardized list of Board self-evaluation questions, some areas that should be considered are:

- the Board's role in building and reinforcing risk culture,
- an understanding of financial and non-financial risks at the Board level,
- the Board's use of risk reporting, including challenge of management's assessment of risks or the basis thereof,
- the Board's interaction with the risk function and management in evaluating the quality and quantity of risk reporting it receives (seeking additional, clearer, or more useful information as needed),
- Board focus on strategic and emerging risks, including acquisitions and new products,

- Board support for the risk function, including provision of IT and human resources, and
- the Board's role in reinforcing the message that risk is everyone's business.

Some questions used by one firm in its Board self-evaluation are included in the *Example of Practice*.

3.6.1 Example of Practice - "Top Ten" Board Self Evaluation Checklist

Board self-evaluations should focus not just on the "hard" questions about whether all material risks are being covered and the quality of risk reporting. The more difficult aspects of deriving actionable results from Board self-evaluations are to determine why, for example, all material risks are not being covered during Board or committee meetings. The reason could be insufficient reporting, a lack of true understanding of the firm's major risks by the Board, or a disproportionate focus on new or fast-growing businesses.

Each of these reasons, which themselves only cover some of the possible explanations for the problem, require different solutions. It is this "soft" side of the analysis that is the most difficult. The danger is that if the true nature of an issue is not diagnosed, not only is it unlikely that the underlying problem will be solved, but the firm and the Board could waste both time and financial resources without any resulting improvement in Board performance. Developing an action plan to remedy any shortfalls in Board performance is the ultimate objective of any self-evaluation; however, careful and thoughtful analysis of the results of the self-evaluation is needed before hastily undertaking remedial action.

"Top Ten" Checklist

1. Has every material risk been allocated to a Board committee, and does this risk have a material amount of time and information allocated to it at each meeting?
2. Are the risk committees, or Board committees that deal with risk, diversified, with a majority of highly experienced expert members?
3. Are the reports from the Board committee on risk understandable to the entire Board, and is there a good interaction between the Board and the Committee Chair on the risk aspects?
4. Is there a short (2-3 pages) executive summary of the material risks ranked by priority and their potential implications for the Board, and, similarly does such a summary exist at a more detailed level for each Board committee? Is there also a more detailed report, with quantitative and qualitative data compared against the Board approved risk appetite?
5. Is there an annual discussion of the Board on emerging risks and the risks outside of normal monitoring or recent conditions? These emerging risks have often proven to be the most dangerous.
6. Does the Board have annual training in risk and its impact on capital and the business in terms of reputation and ongoing growth?
7. Does the Board look at disaster scenarios seriously? Do members know what might kill the firm or do irreparable harm?

8. In reviewing risk, does the Board meet with the business units that commit the firm to the risk in addition to the senior management? Does the Board communicate the risk appetite and limits of risk clearly to these business unit risk takers?
9. Is a disproportionate amount of time allocated to the risk of new ventures and new geographic expansion, especially outside of the normal business of the firm's experience?
10. Is a disproportionate amount of time allocated to fast-growing businesses, no matter what the capital allocated to the business is?

Once the Board self-evaluation is completed, the real challenge is analyzing the results and developing an action plan to strengthen Board risk management and governance. Knowing what the Board's areas of weakness might be is not very helpful without delving into where and why change is needed. The following list of warning signs highlights some of the response that could help pinpoint specific areas of focus.

Does the Board react decisively when the response to a risk question is any of the following?

1. "Every other competitor is doing this."
2. "There is no risk to the firm, as it has been transferred to a third party."
3. "The (regulator/rating agency/customer) does not mind, as they have not said anything."
4. "The risks are fully hedged."
5. "The risks are manageable without a detailed explanation and scenario examples."
6. "The risk metrics, which are modeled, are within the risk appetite but at the upper end of the range."
7. "It has not happened in (twenty/thirty/forty) years, or since the 1930s."
8. "Closing out the position to be within the risk limit will result in an immediate loss, and it is sure to recover next (quarter)."
9. "We need this concentration of (risk/product/asset/liability) to be (competitive/maintain growth/meet plan)."
10. "We have a higher (yield/return) with less risk."

These responses tend to indicate a superficial analysis of risk, and, in particular, a lack of rigor in assessing risk against the firm's strategy, business model, and risk appetite. More pertinently, the responses all point to the lack of a challenge culture at the Board level. Combined with an analysis of the Board self-evaluation, the presence of these warning signs can be used as a diagnostic tool to develop an action plan to strengthen risk governance at the Board level.

SECTION 4. GOVERNANCE AND ORGANIZATIONAL STRUCTURES—ROLE OF THE CRO

4.1 OVERVIEW

The Institute recommended in its CMBP report (2008)³¹ that firms should assign responsibility for risk management to a senior-level officer, in most cases the CRO, who should have sufficient status, seniority, voice, and independence from line business management to have a meaningful impact on decisions. However, in strengthening the role of the CRO, it is important that the function does not come to be seen as a silo that deals with risk in a way divorced from the rest of the business, or that the CRO's responsibility supplants front-line accountability.

Particular emphasis was placed on having the CRO engaged directly with risk committees of the Board on a regular basis, and on regular reporting to the full Board to review risk issues and exposures. It is considered essential that the CRO have direct access to the Board or the Board risk committee in some form, whatever the official reporting relationship or Board structure.

Regulatory reform proposals in the aftermath of the financial crisis also have made similar recommendations, including the Basel Committee's *Principles for Enhancing Corporate Governance* and the Dodd-Frank Wall Street Reform and Consumer Protection Act ("Dodd-Frank"). Recent rulemaking³² implementing Dodd-Frank inter alia requires the appointment of a CRO who reports directly to the risk committee and the CEO.

The IIF - Ernst & Young Survey (2012) indicates that the responsibility and influence of the CRO has continued to expand and that most have an active role in strategic and planning decisions. CROs are generally involved in decision making, from new products to strategy. Evidence of the influence of the CRO is found in reporting lines, with more than half of the firms surveyed reporting that the CRO reports to the CEO and almost all reporting direct access to the Board. Respondents said that it was vital for the CRO to have the support of both the CEO and the Board for risk initiatives. A clear mandate is key to ensuring that the CRO's opinion carries weight in discussions with the business, regulators, and other stakeholders.

Strengthening the role of the CRO cannot be accomplished simply by getting the risk governance

structure and reporting lines right. The foundation of the firm's governance should be the premise that the ownership of risk rests squarely with the business. The next step is to ensure that risk, and specifically the CRO, has an influential voice in management decisions. Once these prerequisites are in place, the firm can structure the CRO reporting line to reinforce and institutionalize its approach to risk governance. Some of the key challenges in implementing risk governance structures include:

- ensuring that fundamental ownership of risk resides in the business, not in the risk function,
- defining the CRO's role in decision making,
- deciding on the optimal balance of technical vs. business expertise for the CRO, and
- structuring the CRO's role and reporting line to reflect the organization's governance structure while ensuring the CRO's stature and authority.

4.2 IMPLEMENTATION CHALLENGE - OWNERSHIP OF RISK

Effective risk governance requires that the ownership of risk and accountability for risk are clear. Regardless of how an organization delineates risk responsibilities, the guiding principle is that ownership of risk clearly resides with the business. This involves more than putting into place risk governance structures, policies, and procedures. Ingraining the belief that risk is everyone's business requires positive and negative reinforcement of desired risk behavior.

Risk Governance Responsibility

Defining ownership of risk begins with a clear delineation of risk responsibility that starts with a formal statement of risk principles owned and approved by the Board. The CRO is responsible for the development and implementation of the risk principles, but it is the CEO or senior management who are accountable for risk taken in their division, even if that risk is delegated to other layers of management in the firm. Risk governance responsibilities should be explicitly assigned to management, and escalation paths to senior management, the risk committee, and, ultimately the Board should be equally clear. Senior management is ultimately responsible for supervising and overseeing all risk.

³¹ CMBP report, 9

³² See *Enhanced Prudential Standards and Early Remediation Requirements for Covered Companies*, 77 Fed. Reg. 594 (Proposed Jan. 5, 2012).

Accountability

Ownership of risk by the business and ensuring its accountability for risk are among the greatest challenges in risk governance. The risk function has an important orchestration role, which includes playing a leading role in establishing the risk appetite and the risk management frameworks, as well as monitoring and aggregating risk. However, neither the risk function nor the CRO “owns” risk, nor can either be involved in policing every risk decision made throughout the organization. Ownership and accountability for risk ultimately lies with the front-line business.

The accountability of the risk taker (the front office or the line business) for adherence to the organization’s risk appetite and risk management policies and processes should be at the core of the firm’s risk governance framework. Ensuring that the business proactively takes ownership of risk, includes risk considerations in day-to-day decision making, and demonstrates alignment of risk taken with the firm’s approved risk appetite can be challenging.

Inherent in embedding ownership of risk in the business is the concept that approval of a risk by the front office implies full acceptance and accountability for any losses incurred. The role of the risk function is to take a wide view of risk, provide an independent perspective without being driven by P&E targets, and help ensure that risks are taken using common sense and good judgment. The risk function’s approval is seen as a positive statement, but ownership of risk, reward, and losses should reside firmly within the business.

Risk-Based Performance Management

The link between ownership of risk and accountability for risk taken can be reinforced through the firm’s performance management framework. Individual responsibility for risk can be reinforced via both positive and negative signals about risk behavior communicated through risk-based performance measures. Just as the firm’s compensation practices can be aligned with its desired risk culture behavior, individual performance indicators can be used to strengthen the business ownership of risk.

Three Lines of Defense

Many firms use a *three lines of defense* concept, with line management being the *first line* of defenses, as it has primary responsibility for day-to-day risk management. Line management responsibilities include ensuring that risk standards, policies, and procedures are adhered to. It is also management that is responsible for the primary identification, evaluation, and management of significant risk. This reinforces accountability for risk management with the risk takers.

The risk function is the *second line* of defense and assures that the requirements of the risk governance framework are met. Second-line risk management roles include:

- identification,
- measurement,
- approval, challenge or escalation, and
- reporting of risk.

The *third line* of defense is internal audit; it is audit’s responsibility to test the effectiveness of controls and the risk governance framework.

Risk-Function Budget

Another difficult question is the allocation of the risk function budget. Some firms and supervisors are unequivocal in requiring that the risk budget be independent of the business units. However, other firms believe that the business must own risk and that this is not possible if the risk function budget is not allocated to the business units. In its CMBP report, the IIF recommended that firms should ensure that adequate resources, including personnel, data, and access to information necessary to assess risk, are allocated to risk management. The IIF also suggested that there should be careful consideration of costs and benefits, taking into account the firm’s size and mix of business.

What is clear is that allocation of the risk budget to the business units can cause some tension on both sides, with the business sometimes resisting risk charges perceived as being too high. The decision on how to manage the risk budget ultimately comes down to the organization’s governance structure and the extent to which the risk function is integrated into the business. If the organization has a mature risk culture and the attitude that risk is everyone’s business is ingrained, the question of allocation of the risk budget may not be as contentious an issue.

4.2.1 Example of Practice Use of Individual Risk-Based Key Performance Indicators (KPIs)

One way to make the concept of ownership of risk by the business tangible is by factoring risk into performance management, in particular using individual risk-based KPIs. One firm sets specific KPIs for all risk-taking employees who have a significant impact on its risk profile. These KPIs are both financial and non-financial and are aligned with the strategic plan. Some examples of KPIs for employees are:

- no overdue audit items or audit reports rated "insufficient",
- no breaches in regulatory liquidity limits,
- no breaches of VaR or event risk limits, and
- meeting the loan to deposit ratio target.

Risk-based KPIs are mandatory for all employees who have a significant impact on the risk profile of the firm, and it is the risk function, not business management that assesses performance. The risk KPIs represent a certain percentage of the employee's performance appraisal score. This percentage weighting can be adjusted, so if the firm believes that risk must be emphasized the risk-based KPIs can have a greater impact on the overall appraisal score – and, consequently, on remuneration. In this way, employees have a strong incentive to align their behavior with both the financial profit or revenue targets, and the risk appetite.

These individual risk-based KPIs are generally aligned with those used by a firm in its risk-based compensation policies. That does not imply that all risk-based KPIs are punitive, as they can be equally valuable in reinforcing "good" risk behavior. The primary objective of KPIs should be to clearly link individual performance to ownership of risk.

4.3 IMPLEMENTATION CHALLENGE – CRO'S ROLE IN DECISION MAKING

It is crucial that the CRO has sufficient status and seniority to influence decision making within the firm. A CRO should have the stature to have an impact on decisions affecting the bottom line. A shift in attitude may be required at all levels of the firm to see the CRO as someone who can positively contribute to profits, and not only act as a constraint on the business. A test of the CRO's seniority and influence on decision making might be to ask when was the last time the CRO's opinion was fundamental in stopping something material from happening or fundamentally changed a core decision.³³

Stature and Seniority

To interact effectively and meaningfully influence the Board, Board risk committee, and other members of the firm's senior management team, the CRO should have the ability to clearly and convincingly communicate risk issues. The CRO's formal title and position are important, but the personal characteristics to persuasively make a case against a decision strongly supported by the business are equally essential. This challenge role is central to the risk function. What is clear is that the CRO cannot be seen as the "police", nor have the primary responsibility for risk control. If risk is seen as being a compliance role, the CRO may in practice be excluded from decision making.

Role in Strategic and Business Decisions

The CRO has a role to play in strategic and business planning, and as these functions have traditionally been seen as the responsibility of the CEO and the CFO, coordination and a strong working relationship among the senior management team is crucial. This is especially important to ensure that risk input is taken into account early in the process. This goes beyond the annual planning process to include acquisitions, the introduction of new products, and large expenditures, such as IT projects. Equally important, an effective CRO needs to leverage strong interpersonal skills to influence and impact organizational risk efforts. It is the CRO who is likely to be the primary risk spokesperson when high-level business decisions are first being discussed.

CRO Veto

As part of senior management, and frequently a member of the Board, the CRO's concerns, opinions, and recommendations should be considered in business decisions and not just limited to risk issues. An open question is the extent to which the CRO should be able to override business decisions based on risk concerns. The value of the CRO having a veto is seen differently across firms and can be a reflection of the firm's governance structure, risk culture, and business model. If the business takes ownership and accountability for risk and the organization's risk and challenge culture is mature, the CRO probably will not be faced with a decision of whether to exercise a veto. It also could be argued that the root cause of any

³³ See International Corporate Risk Oversight Guidelines, ICGN Corporate Risk Oversight Guidelines, October 2010. Pg. 14.

4.3.1 Example of Practice – CRO Veto

One slightly contentious question is that of a CRO veto. Whether the CRO has a veto and when or how it is exercised can be indicative of the CRO's role in decision making. Most CROs would likely agree that if they had to exercise their veto frequently, they may not have the influence needed to truly impact decision making. The power of the veto is that it usually results in escalation of the issue and can thereby help to counteract the strong influence of the business. Any escalation of a risk issue, by formal veto or otherwise, should lead to a serious discussion of the CRO's concerns.

Some firms believe that it can be useful for the CRO to have a veto as part of the risk governance model. In one firm, the use of a veto varies depending on whether the CRO is a member of a local or subsidiary risk committee or sits on the group risk committee. At the subsidiary level, CROs have the right to escalate decisions of the local risk committee to the group risk committee. In this firm, CROs chair the risk committees at all levels, and in practice, policies or transactions not approved by the CRO are unlikely to win the support of the risk committee as a whole. For this reason, it would be rare for the CRO to exercise a veto at the group risk committee level.

Other instances where a veto might be used are in the approval of new products, or on defining risk-based materiality thresholds for transaction limits and reporting. It is important that the CRO veto not be used in the same way that compliance might disallow a transaction due to legal or regulatory concerns. Risk-based vetoes should be an opportunity to address the broader implications of certain actions in the context of the organization's risk culture and risk appetite.

Other firms believe that a challenge culture and a decision-making process that favors compromise is more productive than a formal veto. These firms take the approach that the CRO should be an equal member of the senior management team and as such should wield enough influence that a formal veto is not required. If the CRO is someone whose business judgment is valued, the question of a formal veto becomes less important. What is critical is the full participation of the CRO throughout the decision making process, not the exercise of a veto after the fact.

situation in which a veto might be required is the firm's governance structure or its risk management framework. If so, these may need to be strengthened to deal with similar issues in the future, rather the exercise of a one-off veto that probably will not have a lasting impact on the firm's approach to risk.

Advisory Role

One of the elements of the CRO's responsibilities is acting in an advisory role to the Board, keeping the Board informed of, and opining on, the firm's risks. This advisory role should not undermine the CRO's ability to have a meaningful impact on decisions that affect the firm's bottom line, and this can be reinforced by fostering a close working relationship and ongoing cooperation with both the CEO and the CFO. Balancing risk management responsibilities, with the advisory role is crucial to strengthening the role of the CRO. The CRO's advisory role generally encompasses:

- driving the firm's risk culture,
- opining and advising on the firm's risk appetite, risk framework, and risk reporting,
- advising the Board and the CEO on key and emerging risks, and
- coaching the senior management team on risk.

The CRO should have a strong understanding of, and be able to focus the Board's attention on, the firm's top risks. The Board needs to be properly informed of the firm's risks, but part of the CRO's responsibility is to prioritize and know which issues do not need to be escalated to the Board.

Trying to find the right balance between the CRO's advisory role to the Board, in the sense of providing input and helping to frame decision making on key risk measures, and being part of the senior management decision making team is an ongoing subject of discussion in some organizations.

4.4 IMPLEMENTATION CHALLENGE - TECHNICAL VS. BUSINESS EXPERTISE

Both technical risk management expertise and a sophisticated understanding of the business are essential for the CRO to be able to effectively influence Board and business decisions. Combining these two characteristics in one person is not easy, and firms may need to strike a balance between the two. Determining the optimal mix and then finding the right person is not always straightforward.

4.4.1 Example of Practice – Technical vs. Business Expertise

For the reasons discussed previously, some firms prefer to appoint CROs who are internal business managers with sufficient affinity for risk management, as opposed to hiring an external risk manager. The belief is that it takes longer for an external risk manager to gain in-depth knowledge of the organization's culture, get acceptance as change manager, and be able to challenge top management, than it takes for an internal business manager with the right background to acquire the necessary technical knowledge. One firm found that an existing policy to rotate senior managers in the context of succession planning could be useful in sourcing internal candidates with the right profile to become CROs.

One firm is wary of a heavy reliance on models, which it believes can be a result of an over-emphasis on technical skills in the risk function. In this firm's opinion, the excessive faith put in models and the lack of common sense applied in evaluating the assumptions driving the models were major problems during the recent crisis. Further, there is a concern that an over-reliance on models and technical expertise at the expense of business experience in the risk function can contribute to an arbitrage culture. The firm emphasizes that common sense and judgment are crucial for the CRO to interpret and put into context the technical output of models used in risk management. This firm values a CRO who has enough knowledge of the business to be able to understand the financial motivation driving, for example, new product decisions.

Another firm follows a two-pronged approach to engage the CRO in risk decision making. First, the CRO might be asked present a business opinion on a particular deal, product or transaction. As a second step, the CRO could then add the risk preconditions for completing the transaction. In this way, the CRO has input into the business decision based on experience and judgment, yet also has the opportunity to raise the risk implications or concerns.

Demonstrating an understanding of the business motivation of a transaction in this way can help build the CRO's credibility, and this credibility can then be leveraged to enforce the risk caveats raised. Of course, the limitations of this approach should be considered, as the CRO's role is not to second guess business decisions or to act as the first line of defense. As suggested earlier, a certain amount of healthy tension between the business and the second line of defense function may contribute to better risk decisions.

Whichever approach is taken, firms should ensure that the required technical risk management expertise exists within the risk function. The more technical aspects of risk management experience do not necessarily need to reside in the CRO. However, depth of experience in, for example, monitoring and testing risk controls, is needed in the risk management area. As discussed here, the CRO of highly complex organization should be fully conversant with risk management principles and practices. The appropriate balance between technical risk management experience and business expertise largely depends upon the nature, scale and complexity of the firm's business.

Considerations in Balancing Technical vs. Business Expertise

The firm's governance structure, the maturity of its risk culture, and its business model are factors that can influence the decision to appoint a CRO with predominantly technical risk management or business expertise.

As part of the senior management team, led by the CEO, the CRO takes on different roles including independent challenger, trusted adviser, and culture change manager. The incumbent has to be able to combine business expertise with technical risk management knowledge to take on these diverse responsibilities. To have their advice and opinions solicited and implemented by their colleagues, CROs should be knowledgeable about the organization's business and culture in general, and its risk profile and risk culture in particular. As previously discussed, the CRO also needs to have the stature and ability to go against business heads or even the CEO when calling a "time out" is needed.

Minimum Technical Expertise

In its notice of proposed rulemaking, Sections 165/166 of Dodd-Frank,³⁴ the U.S. Federal Reserve asked if minimum qualifications should be specified for a CRO. One requirement might be to require CROs to have experience in monitoring and testing risk controls. In calling for formal, professional qualifications for CROs, stakeholders should be mindful of the different aspects of the CRO's responsibilities. Although the CRO of a large and complex global financial institution should be fully conversant with risk management principles and practices, having the ability to implement a risk framework tailored to the nature and scale of the firm may be more relevant than direct experience in a risk-control function.

³⁴ *Enhanced Prudential Standards and Early Remediation Regulations under Dodd-Frank 165/166*, Pub. L. No. 111-203 (2010).

4.5 IMPLEMENTATION CHALLENGE – CRO ROLE AND REPORTING LINES

Different Board structures, business models, and regulatory requirements mean that there is no “one” model for CRO reporting lines. The difficulty lies in ensuring that the CRO has the required access to the Board and senior management to ensure input on risk issues at an early stage in strategic and business decision making.

The CRO's Role

The CRO's role usually encompasses oversight of the firm's primary risks, such as credit, market, funding, and liquidity risk, as well as operational and reputational risk. Risk governance responsibilities include being the chief proponent of the firm's risk culture, using every reasonable opportunity to bring risk issues to the attention of the Board, Board committees, senior management and the business. The CRO is likely to take an active interest in promoting and implementing the firm's risk training and risk-based compensation policies to reinforce the desired risk culture. Any efforts to strengthen the firm's challenge culture and ingrain ownership of risk with the business will be driven by the CRO on an operational level.

As the head of the risk function, the CRO is normally charged with designing and overseeing the risk governance framework and assisting the Board or Board risk committees in defining the firm's risk appetite. In summary, the CRO is responsible for supporting the business in all aspects of risk management. This does not imply however, that the CRO is solely responsible for the operation of the risk management framework, as the business is the first line of defense and has primary responsibility for day-to-day risk management. One model is to hold the CEO, CFO, and CRO jointly responsible for the implementation of the risk framework agreed upon by the Board, with ultimate accountability resting with the Board, whether directly or via its risk committee.

CRO Reporting Line

The CRO should report to as high a level as possible, but should maintain a connection to the line business. In some organizations, the CRO has a matrix reporting line to the business, and through the risk function. In firms with diverse business lines and multiple locations operating in different jurisdictions, a matrix reporting structure is unavoidable, despite the possible dilution of risk responsibility this may cause.

Development of the Risk Framework

In many organizations the CRO is responsible for the development and implementation of risk principles and the risk framework. The development of the risk framework is often one of the CRO's central responsibilities. Such responsibilities may include outlining how risk is identified, measured, and monitored, as well as approval of transactions, positions, exposures, and provisions. Implementing the risk framework involves not just initially defining the framework under which the organization operates, but also updating it in a constantly evolving financial market. In developing and maintaining the organization's risk management framework it is important that Boards, senior management, and the CRO keep in mind that:

- It is unlikely that any framework will be fully able to anticipate all innovations in financial markets and products.
- Any risk management framework has the potential to be arbitrated and should therefore include some high-level principles in addition to “hardwired” processes, procedures, and limits.
- The risk function has to be engaged in material acquisitions, new products, deals and transactions before they are completed. This is to ensure that risk is able to voice any concerns in advance and potentially stop the process if required.
- Models are not infallible, and judgment is needed in decision making.

Finally, it is important to acknowledge that any framework developed will not prevent the next crisis. A good risk management framework that is part of a strong risk governance structure may, however, make it easier for the Board, senior management, and the risk function to see problems developing earlier, respond sooner, and perhaps minimize the negative consequences.

In addition, regulatory expectations may differ across jurisdictions. In some jurisdictions, there is an expectation that the CRO report directly to the Board or Board risk committee. Balancing legal, regulatory, and other stakeholder expectations against the organization's corporate structure and business model can require careful management of the governance process. The CMBP report notes that the CRO's reporting line is commonly to the CEO, and that there is frequently an obligation to advise the Board and Board risk committee of significant issues.

4.5.1 Example of Practice – CRO Role and Responsibilities

Some firms believe that centralizing the risk function under one CRO improves efficient group-wide risk management and, therefore, they have the CRO report to, or have access to, the group Board. Other firms believe that risk is better controlled at the local level, and CRO reporting lines and access to the Board reflect a decentralized structure. For still other firms, one of the advantages of appointing local CROs is that risk management can be brought closer to the business.

To fully incorporate risk into strategic planning at an early stage, CROs often have a seat on the committee responsible for developing the firm's strategic plan. An important role for the CRO in the planning process can be to ensure alignment with the firm's risk culture and risk appetite. Many CROs are members of the compensation committee, where their input can be crucial in reinforcing the firm's risk culture. In some cases, the CRO has a reporting line to the Board audit committee, to provide an alternate avenue for the risk function to escalate risk issues to the Board level, if required.

Many firms emphasize the CRO's role in capital management by having the CRO sit on the committee responsible for capital allocation. This approach has been adopted both at firms that have a centralized business model with one group CRO, as well as at those that have a decentralized structure with several local CROs. One firm describes the CRO's role as ensuring that the business operates within its "risk and capital playing field". The objective is for the CRO to be involved in capital planning from the beginning of the process, thereby avoiding the need to modify or reverse capital allocations based on risk considerations.

To integrate risk into the day-to-day business, the CRO's role cannot be limited to development of the risk framework, advising the Board on risk appetite, or being the guardian of the firm's risk culture. The CRO's role should be ingrained in the firm's governance structure and institutionalized to make risk consideration an integral part of the firm's operations. Exactly how this is best accomplished may vary from firm to firm and should be adapted to the particular risks faced by the firm as well as its governance structure and business model.

CRO Access to Board

Some firms consider it essential for the CRO to have a seat on the Board to be independent. Ideally, the CRO should have high visibility on the Board and, at a minimum, the CRO should have access to the Board or Board risk committee. It is important that the CRO be able to raise risk issues at the Board level without going through the CEO.

Relationship with the CEO

Many firms find that the relationship between the CEO and the CRO is critical to how risk issues are handled. One firm characterizes the relationship between the CEO and the CRO as one of "constructive tension." Others believe that the CEO and CRO should complement each other, but take a different approach – "do things in a different way". Regardless of how firms resolve the CRO's reporting line and relationship with the CEO, risk decisions should be based on the judgment of the CRO within the framework of the organization's governance structure and challenge culture.

Hiring, Firing, and Compensation

The question of who is responsible for the hiring and firing of the CRO also should be considered. Hiring and firing of the CRO should, at a minimum, be in consultation with the Board or Board risk committee, if not at their sole discretion. As the CRO is a member of the senior management team, the CEO should at the very least be expected to explain any hiring or firing decision to the Board or Board risk committee.

The Board should likewise have a role in setting or reviewing CRO compensation. There is no one approach in the industry on the question of CRO compensation and the extent to which it should be flexible or risk-based. To attract the best people and raise the stature of the CRO position, some form of performance based pay seems warranted. However, just as many firms are still struggling to implement true risk-based compensation for non-risk staff, CRO risk-based remuneration is a work in progress. Whichever approach a firm takes, the importance of CRO compensation should not be underestimated in ensuring the independence of the risk function.

CONCLUSION

The financial industry is conscious of the importance of further strengthening risk governance. While there has been a focused effort across the industry to embed lasting improvements to the governance of risk, some challenges remain. There is common agreement on the need to build a strong risk culture, develop a robust risk appetite framework, increase the Board's role in risk governance, and strengthen the role of the CRO. None of these recommendations are disputed; however, the question of how to do this in practice is less clear. As the Examples of Practice included in this report show, firms are making progress in embedding risk culture, cascading risk appetite, and defining and strengthening Board risk committees, but challenges remain on how to produce lasting improvements.

Strengthening a firm's risk culture is crucial. However, it should be recognized that a strong risk culture cannot be developed in a short period of time. Risk culture needs to be an integral part of the organization's wider corporate culture, and both corporate and risk cultures are developed over the long-term and need to be reinforced through the day-to-day signals sent by management and by ongoing training. There is no quick fix to strengthening risk culture. Instead, the focus should be on truly embedding improved risk governance throughout the firm.

A robust risk appetite framework is key, and although a risk appetite framework may be developed quickly out of necessity, once developed it needs to be ingrained in the way the organization thinks about and acts regarding risk. Just as the risks facing organizations change continuously, resulting in changes in strategies and business plans, the risk appetite framework must be a living document that is updated to reflect changes within the firm and in the wider macro-economic environment. Developing and implementing this risk appetite framework is an iterative process, and it is this process of continual improvement that allows the organization to respond to the changing economic, business, and regulatory environment.

Increasing the risk role and responsibilities of the Board, Board risk committees, senior management, and the CRO are areas rightly receiving a great deal of regulatory

attention. Although there are basic principles that can be applied to all organizations to improve risk governance by clearly outlining the responsibilities of the various players, this is the area in which the most caution is warranted. It is correct that certain principles are universally applicable – for example, that risk governance is the responsibility of the whole Board, or that the CRO should have sufficient seniority to influence decisions. However, it is also an area in which allowing firms discretion on how, but not if, these principles are implemented in practice is important.

Just as a strong risk culture cannot be bolted onto a weak corporate culture, "one-size-fits-all" requirements for risk governance roles and responsibilities cannot be superimposed on firms, as this is not likely to create concrete and long-term improvements in risk management. Firms operate in various jurisdictions and different markets and under divergent governance structures. Without allowing a tailored approach to risk governance, stakeholders may be undermining the ultimate objective of risk management—achieving a balanced risk/reward equation. In developing risk governance structures, firms should have the discretion to adapt risk governance principles and requirements to build on their organizational strengths and remedy any weaknesses.

ANNEX I. ADDITIONAL EXAMPLES OF PRACTICE

THE ADDITIONAL EXAMPLES OF PRACTICE INCLUDED IN THIS ANNEX REPRESENT THE EXPERIENCES OF INDIVIDUAL IIF MEMBER FIRMS AND ARE NOT NECESSARILY REPRESENTATIVE OF THE FINANCIAL INDUSTRY AS A WHOLE. THEY ARE INTENDED TO SERVE AS ILLUSTRATIONS OF HOW ONE FIRM HAS DEALT WITH THE IMPLEMENTATION CHALLENGES OF STRENGTHENING RISK GOVERNANCE.

SECTION 1. RISK CULTURE

EXAMPLE 1. RISK CULTURE AUDITS – HOW DO THEY WORK AND ARE THEY EFFECTIVE?

The problem that needed to be addressed:

Risk culture is now seen as a key contributing factor to the global financial crisis. Thus, financial services firms are beginning to acknowledge the need to embed a 'strong' risk culture – one associated with effective communication around risk expectations, understanding of risk appetite, appropriate incentives, and enhanced decision making – to mitigate against further crises of this sort.

Interest in potential approaches for measuring, evaluating, and monitoring risk culture is growing, and many companies are seeking valid processes and tools for auditing their risk culture just as they would audit other aspects of their business.

Risk culture is defined by people's understanding of, and attitudes toward, risk, which is manifested in risk behavior. An audit of risk culture, therefore, seeks to assess management's and employees' understanding of, and attitudes toward, risk within their organization. A risk culture audit will allow management, risk functions, and audit functions to:

- Identify any gaps between the desired and actual risk culture.
- Clarify areas of priority for further testing and potential intervention.
- Identify Key Risk Indicators (KRIs) for management.

How this firm went about addressing it:

Creating a Risk Culture Audit Approach:

Creating an effective risk culture audit approach requires careful thought and planning. In many cases, management may identify the need to review risk behavior following an event or report of problems (e.g., from whistle-blowing or staff opinion surveys). In other cases, the need to survey and monitor risk attitudes may be driven by the risk function or audit function as part of a general program to improve risk management.

In an audit, the actual risk culture is assessed against the desired risk culture. Once the gaps have been identified, a culture change program can be developed and implemented.

The typical approach for auditing risk culture within a financial services firm is as follows:

Step 1– Leadership assessment:

- The first step is to meet with leadership to establish the desired risk culture, including strategy, risk appetite and controls.
- The assessment should include broader strategic questions as well as more-focused questions that target specific cultural risk factors that may be unique to the organization or based on a validated risk culture model.

Step 2 – Individuals' perception of risk

- The second step is to assess individuals' understanding of, and attitudes toward, risk, using a self-report questionnaire.
- The questions should be derived from a comprehensive model of risk culture, assessing such factors as governance, decision making, and competencies. When off-the-shelf tools are used, the questions may need to be tailored to account for different approaches to risk

within different subsectors and across organizations.

- Responses are analyzed to understand how the factors interact and to identify areas in which risk culture is not aligned to risk appetite.
- It may be appropriate to analyze the questionnaire results according to different demographic groups. One way of analyzing results may be to look at how they vary across risk owners, risk controllers and risk takers.

Step 3 – Reporting

- Results are presented to leadership, highlighting gaps between actual and desired risk behavior for each of the risk culture factors.
- The outcomes of the assessment are discussed with management and other functions, as appropriate; to explore the potential causes of any misalignment of risk culture and prioritize areas for change.
- Results also may be shared with employees to ensure a collective understanding of risk issues and gain buy-in to the change process.

Step 4 – Action plan

- The final step is to develop an action plan to achieve cultural change.
- The action plan should outline specific activities to effect change, including responsibilities and measurements for success.
- Examples of actions that may arise out of a risk culture audit are:
 - More frequent and clear communication from leadership on the organization's risk appetite and tolerance.
 - Mandatory training for all staff on the organization's risk management policies and processes to enhance decision making.
 - Review of the performance management framework to incorporate risk behaviors.
 - Review of variable remuneration structures to ensure inappropriate risk-taking behavior is not incentivized.

Key Lessons:

- The risk function should manage the audit and act as liaison between the business and senior management.
- An effective way of gaining acceptance of the proposed risk culture model and audit approach is to pilot the audit within the risk function before rolling it out to other business units.
- Creating simple, easy-to-understand outputs with clear business application will help gain commitment to the results and action plan.

- It is important to emphasize that there is no such thing as a "good" or "bad" culture, only one that is aligned or misaligned to the organization's broader risk strategy and appetite.
- Cultural change is a long process that requires full support from leadership and involvement across all levels of the organization. The action plan should include "quick wins," with tangible benefits, to secure commitment to the change process.
- In global organizations, it is important to understand the cultural norms within each jurisdiction before assessing the risk culture. The approach will then need to be tailored to account for these cultural differences.
- The risk culture audit should be repeated at regular intervals to assess the effectiveness of any cultural change initiatives.

EXAMPLE 2. RISK CULTURE AUDITS

The problem that needed to be addressed:

Risk culture has been identified as a key differentiator between peers in the financial industry. The understanding and framework through which risk is managed in the firm should be strong at all levels and in all functions throughout the organization. Improving risk culture is a key objective across the industry, marked by an increased focus on communication, training, accountability, and measurement.

How this firm went about addressing it:

- A bank initiated a group-wide Risk Culture Initiatives program in 2010. This program's scope was defined and validated by senior management from all divisions. Its key objective is to drive measurable improvement in the firm's risk culture. It was decided that this was to be done through ongoing management and measurements versus ad-hoc audits, which might be considered in the future. As a first step, the program established core risk culture behaviors which all staff are expected to exhibit. The central theme of these behaviors is the expectation that everybody— not just the risk management department—is responsible for managing risk, and that risk must be managed in a way that protects the reputation of the firm and supports long-term sustainable financial performance. The risk culture behaviors are included in firm's key policies, such as the Code of Conduct, as well as in the internal performance management tool to ensure that managers evaluate their staff against both their deliverables and their risk behavior.
- To further ensure that these behaviors are embedded in the organization, a number of parallel initiatives were implemented:
 - Constant and consistent communication and tone from the top messages
 - The development of a comprehensive risk culture training program that was rolled out to all levels of the organization and included more in-depth training for employees being promoted to Director or Managing Director level. Many of the training courses are mandatory and include tests that employees are required to pass.
 - The implementation of a process to provide early vetting of transactions that display a risk profile outside generally accepted parameters is consistently used across the investment bank.

Key Lessons:

Six critical success factors have been identified since launch of the initiative:

- Strong support for the initiative from senior management is critical in terms of both tone from the top and in terms of driving targeted programs through the businesses.
- Constant communication to staff and tone from the top messages that emphasize that everyone is responsible for managing risk. These messages are most powerful if they come directly from the divisional management and not from the risk function. This area needs constant attention and updating.
- Clearly linking expected behavior to performance reviews, compensation, and promotability has proved very effective. The results of the quarterly "red flag" process are shared with senior divisional management and are taken very seriously. Targeted communication ensures that employees understand that they are accountable and will be directly impacted by noncompliance. It is important to continue to evaluate the individual measures used to ensure they remain relevant. To further strengthen the link to performance reviews, risk cultural behavior is included in job profiles.
- Simple and transparent measures support the red flag initiative. The suite of breaches that make up "red flags" should be transparent and easily measured, and regular information should be made available to divisional management so that breaches can be actively managed and reduced.
- Data quality of "red flag" breaches must be extremely good or the process becomes entangled in a discussion regarding the measurement rather than the outcome. As a result, a shadow process for all new "red flags" going forward will be introduced, which allows the sharing of the data down to the employee level.
- To ensure compliance with supervisory responsibilities, a dedicated "Tone from the Top Red Flag" will be introduced that will further motivate supervisors to ensure they are setting the right tone in their teams.

EXAMPLE 3. AN EXAMPLE OF EFFECTIVE RISK EDUCATION

The problem that needed to be addressed:

Incoherent and unaligned risk training throughout the organization, in conjunction with risk management becoming an increasingly complex discipline, made this bank realize that a more comprehensive and centrally managed approach was required to ensure high-quality risk education. Objectives were to define and upgrade training needs in a coordinated fashion and to optimize internal and external resource allocation, with the aim of creating a talent pool of internal risk professionals. It was therefore decided to establish a Corporate Risk School (CRS) fully dedicated to building quality risk training programs tailored to the needs of the different business units and risk departments, as well as to risk and nonrisk employees.

How this firm went about addressing it:

- The CRS annually redefines training requirements on the basis of strategic risk goals, main challenges impacting the group, and business plans.
- These requirements translate into four areas of training: (1) executive programs; (2) "best practice" programs per risk group; (3) courses tailored to the needs of the various risk disciplines; and (4) open training sessions organized on a rotational basis by the 53 different risk departments. In addition, e-learning is provided to all employees in the group.
- To date, iterative sessions of four main comprehensive risk programs (retail, wholesale, financial risk and overall risk) have been rolled out, taking in virtually all risk executives as well as business unit managers.
- The firm's top 200 employees, as well as the next layer of management, are enrolled in strategic risk programs. An extensive Board training program is attended by executive and non-executive directors.
- In cooperation with renowned universities, the CRS has further established an internal Master in Risk program: a two-year fully certified master's degree open to selected employees from inside and outside risk departments. The program combines internal practitioners' views with academic research by incorporating instruction from internal risk executives and university professors.
- The intention is to have the talent pool of the risk division with between two and eight years of work experience undergo the program.
- The CRS has rapidly expanded through the establishment of 11 local Risk Schools, some of which with a regional coverage.

Key Lessons:

- The firm found that interest in the programs was overwhelming and took much internal organization. The most effective form of communication between in-house sessions has been through internet-based applications and social media.
- The firm also observed that, in addition to developing a high-quality risk management pool, an important side effect of the CRS programs has been the retention of personnel. Risk professionals feel included, with positive effects on loyalty and work satisfaction.
- The emphasis on internally developed, in-house risk training for non-risk employees is seen as a perfect tool to further embed the firm's risk culture in the entire organization.
- The CRS is aware that it must try to increase the number of courses without jeopardizing quality, and must keep abreast of all new developments in risk that could potentially impact risk education
- In this context, there is still some way to go to achieve the right balance between internal and external trainers, as the capacity of senior risk managers to be involved in a growing suite of training programs is already stretched.

EXAMPLE 4. CRO LEARNING AND TRAINING INITIATIVE – RISK ACADEMY

The problem that needed to be addressed:

Financial crises highlight the fact that the success of risk-taking institutions depends upon their risk management capabilities. The key pillars of successful risk management include understanding risk and its effects on P&L and the balance sheet, creating a consistent base level of technical risk knowledge, reinforcing communications at all levels, and creating a mindset that anticipates changes in the macro-environment. It was therefore important for this bank to create a risk learning framework that helps prepare employees for this very challenging environment while also helping to build a stronger and more effective risk culture.

How this firm went about addressing it:

- To strengthen awareness of risk management and deepen the firm's risk culture, the "Risk Academy" was created. This is an initiative developed and managed by a dedicated unit within Group Risk Management Department in cooperation with internal learning and training competence centers.
- The Risk Academy serves as a center of excellence for risk culture and risk training, providing a common and consistent learning approach to risk issues and the risk environment. With the establishment of the Risk Academy expert, know-how joins state-of-the-art learning.
- The Risk Academy has created a multitier risk learning framework that addresses the educational needs of professionals at all levels, with dedicated learning streams available to the entire range of the firm's professional staff.
- The Risk Academy has a global approach. The same learning and training is available to the entire group and includes participants from different legal entities and countries. This further strengthens the idea of a single risk culture and supports a group-wide understanding of major risk concepts and risk know-how.
- Since knowledge of risk and risk culture has several components, the Risk Academy has designed differentiated training and learning programs.

Risk Diploma Path

The Risk Diploma Path comprises an intensive 11-week online Core Curriculum and two online advanced-level Masterclasses of four weeks each. It is open to the professional risk function and all other interested nonrisk-function professionals, such as finance, human resources, and internal audit.

The Core Curriculum provides an introduction to the fundamentals of risk and risk management whereas Masterclasses, which follow the successful completion of the Core Curriculum, are designed to deepen risk knowledge by allowing participants to explore advanced concepts. All courses have been formulated using web-based training modules, which are supplemented by webinar videos, web-training presentations, business cases, and online testing. Successful completion of the Risk Diploma Path results in a Certification issued in cooperation with an internationally recognized university.

The online training is offered in the three major languages of the firm. To date, more than 5,000 employees, on a global basis, have participated in this program.

Strategic Risk Management Learning Labs

The Strategic Risk Management Learning Labs include two days of intensive learning and activities related to various key risk topics. The objective is to enhance, in a clear, nontechnical way, an internal sensibility toward risk; to raise the awareness of core aspects of risk management, risk management's role and its relation with the business and other nonrisk functions and to strengthen key fundamental risk know-how.

Contents include credit risk, market risk, liquidity risk, reputational risk, operational risk, and restructuring, as well as risk governance and risk culture. The approach is based on a learning experience that builds on the principle of peer-to-peer knowledge sharing, and combines expert lectures with activities.

The Learning Labs are offered to nonrisk management senior executives, and 150 executives have already participated in this program.

Risk Master Series

The Risk Master Series approach is built on a state-of-the-art learning experience in which the goal is to strive for a single risk culture. The training modules are designed to:

- Enhance risk know-how and risk professionalism.
- Reinforce the ability to manage complexity and handle critical conversations.
- Improve communication and leadership skills.
- Strengthen the Risk/Business cooperation.

This tailor-made learning path has been designed for senior risk management and business executives and is composed of two modules of two days each. To date, more than 150 executives have participated in this program.

Tailor-Made Training on Demand

Training on demand, covering a day and a half to two days of classroom training, represents a new channel by which the Risk Academy caters to the specific educational needs and requirements of the risk function, the business, and other nonrisk functions. During 2011, the first trainings on demand were developed and delivered on different topics, including Internal Capital Adequacy Assessment Process (ICAAP), project finance, and credit process in foreign branches.

Key Lessons:

- It is essential to implement a Risk Academy within the risk management department so as to take full advantage of expertise and know-how, faculty support and relevant networks.
- It was found to be quite essential to invest sufficient time in marketing and communication (e.g., Risk Academy roadshows have been organized in major venues, close regular dialogue with human resources has been maintained).
- It is very important to have top management support (e.g., for budget issues, instilling the idea of risk culture throughout the firm, and promoting the training offered).

Building, and ultimately strengthening, a risk culture is a *multi-focus, multi-step* process that is *implemented over time* and does not happen overnight. With the Risk Academy an important step has been implemented. Other steps will follow over time, but cannot be rushed or forced. These include building *mutual respect*, developing *credibility*, creating *accountability*, instilling a *common sense approach* to risk management, and creating a *business/risk rotation path*.

All of these form the fabric of a risk culture and must be allowed to develop in the right environment.

EXAMPLE 5. RISK-BASED COMPENSATION PRACTICES

The problem that needed to be addressed:

There are many challenges in designing pay and benefit programs that strike an optimal balance between risk and reward. Performance management systems need to assess employees against short-term business performance goals, and compensation programs typically reward employees for attaining these short-term goals. However, at the same time performance management systems and compensation programs need to promote behaviors and results that are in the long-term interests of shareholders and customers, thereby mitigating or escalating key risks.

How this firm went about addressing it:

Incentive Compensation: High-Level Principles

The first step in developing risk-based compensation programs is to bring clarity to the underlying objectives. For example, high-level principles could include the following:

- Incentive compensation programs align with organizational strategy and culture, and support the short- and long-term success of the enterprise through pay for performance.
- Incentive compensation programs are approved, monitored, and adjusted for risk according to the governance and review processes of the enterprise.
- Incentive compensation philosophy, programs, and policies provide a competitive pay opportunity that allows the enterprise to attract and retain talent.
- Incentive compensation rewards are not guaranteed and are dependent on performance of the enterprise, business units, and employees.

Risk-Based Incentive Compensation: Design Process

Designing a risk-based program is an iterative process that engages stakeholders throughout the organization. The major stages in the design process can be summarized as follows:

- **Needs Assessment:** 1) Assess compensation change need; 2) Review against regulatory requirements; and 3) Identify risk-based plan materiality.
- **Establish Program Parameters:** 1) Review parameters and considerations from an Human Resources, Finance, Risk, and Compliance perspective; and 2) Identify project team.
- **Develop High-Level Design:** 1) Define high-level design elements such as metrics, funding mechanism, and allocation method; 2) Review funding feasibility; and

3) Review high-level design from an Human Resources, Finance, Risk, and Compliance perspective.

- **Develop and Test Detailed Design:** 1) Develop a comprehensive design model; 2) Conduct affordability and sensitivity analysis; and 3) Review and test the detailed design from an Human Resources, Finance, Risk and Compliance perspective
- **Approval:** 1) Obtain concurrence from HR executives; 2) Obtain concurrence from control functions; and 3) Obtain final approvals as appropriate

Establishing Materiality and Designing Risk Compensation Score Cards

- Each business group was made responsible for developing Risk-Compensation Scorecards for their respective lines of business – for material compensation plans only (i.e., materiality based on risk level of the business group and total compensation spending).
- The Risk-Compensation Scorecards account for key market, credit, and operational risk metrics, tailored for each line of business to define risk appetite and tolerance, as well as to influence compensation design and program review.
- For year-end incentive pool reviews, the CRO for each business group provides input. If appropriate, the CRO could recommend adjustments to pools to ensure alignment of risk and return based on results from the Risk-Compensation Scorecards.
- The weight assigned to each of the risk factors varies across business groups and their respective lines of business. Each Risk-Compensation Scorecard is customized specific to the nature, size, and type of business, which is determined by the business group's Operational Risk Officer and CROs.

Key Lessons:

Implementation Challenge #1: Accounting for Difficult-to-Measure Risks

Each business group's Risk-Compensation Scorecard accounts for various types of risk; some groups may weigh reputational and legal risk more heavily. Regardless of the weighing for these particular difficult to measure risks, the Operational Risk Officer and CRO apply acute business judgment for such risks when providing input or recommending adjustments to year-end incentives pools.

Through extensive reporting, the Business Group Operational Risk Officers and CROs are well informed of all significant, emerging, and potential risks, including reputational and legal risks. Potential reputational risk issues are identified, mitigated, monitored, discussed and

escalated as part of existing approval processes within business groups and corporate services areas.

Implementation Challenge #2: Compensation Program Design for Control Functions

Special consideration was given in the design of compensation programs for leaders in control functions (e.g., operational risk management staff as well as other second-line-of-defense functions in the corporate areas). There was a need to establish a tighter link between individual performance and operational risk performance, incorporating explicit operational risk performance metrics into performance evaluations.

The following suite of performance management metrics (based on existing processes) were included in the programs:

- Self-assessment compliance ratings.
- Operational risk loss amounts (vs. tolerances).
- Business environment internal control factor scores used in the Advanced Measurement Approach (AMA) operational risk management methodology.
- Economic and regulatory capital consumption.
- Qualitative metrics (e.g., maturity of the operational risk management framework in a specific area and progress made in closing gaps/advancing best practices).

EXAMPLE 6. COMPENSATION POLICIES TO MATCH RISK CULTURE AND APPETITE

The problem that needed to be addressed:

Compensation policies and practice should reward appropriate risk taking to achieve an appropriate reward, and should never reward risk taking that would materially affect the sustainability of the firm no matter what the potential reward. Executing this in practice is very challenging, especially with complex financial products with risks that are spread over many years and compensation cycles.

How one firm went about addressing this:

- In banking, aligning compensation with a risk limit system has been generally well managed for shorter-term risk products (less than one year), although there have been a few high-profile exceptions, usually involving fraud.
- The challenge in financial services is when the risk for a product is spread over many years and, therefore, many compensation cycles. This is especially true in insurance, where the risk can be material even after a decade.
- Firms can create a risk limit structure to protect on the downside, but getting a good return on risk is an even greater challenge.
- One international specialty property and casualty insurance firm addressed these challenges by creating an incentive compensation system for cash target bonuses (an annual award as a percentage of salary) that measures the business written by an underwriting team for a plan year over a ten calendar year period. Each year of historical business is measured based on actual returns on capital, thereby creating a triangle of capital weighted ROEs.
- The target bonus is paid out at (i) 100 percent if the business produces a 15 percent ROE, which the firm believes is an attractive return to capital providers given the risks it assumes; (ii) at 0 percent if the ROE is less than 8 percent; and (iii) capped at 200 percent if the ROE is more than 23 percent. The plan also incorporates claw-backs and carry-forwards of target bonuses in certain circumstances.
- Payouts in each plan year generally vest 40 percent / 20 percent / 20 percent over the first four years, with subsequent recalculations in years 5 through 10 contributing (or deducting) from that year's cash bonus calculation.

- This is done at a segment level and then cascaded down to each underwriting unit and plan participant.
- This system not only aligns the final reward of the underwriter to that of the capital provider, but also rewards writing more business when ROEs are high and less business when ROEs are low; a critical element for above-average performance in the historically cyclical property and casualty insurance business.
- In addition to this annual cash incentive, senior underwriters receive a long-term incentive award of equity-based compensation that vests over three years.
- An underwriter can retire and payments will continue for the next ten years as long as he or she does not work for the competition.
- This system has worked very well over the last ten years, with successful underwriters earning compensation that has been aligned with the firm's favorable performance over the period.

Key Lessons:

- The best way to match risk appetite and selection to financial reward is to fully align the interests of the risk selector (an underwriter) to the capital provider (senior management/shareholders).
- Timing must be aligned as well, as risk is not uniformly distributed over the life of a financial product.
- Measuring a risk selector's actual results over a long period creates a successful partnership, and has proved to create corporate above-average risk adjusted returns.

SECTION 2. RISK APPETITE

EXAMPLE 7. EMERGING RISK IDENTIFICATION AND ASSESSMENT

The problem that needed to be addressed:

As the risk landscape changes ever faster, a forward-looking, ongoing risk perception survey targeted at employees can be a very useful tool to stay abreast of the latest development in the firm's risk landscape. One insurance firm developed such a survey over ten years ago as an emerging risk identification and assessment tool.

How this firm went about addressing it:

A fast-changing business environment

New economic, technological, sociopolitical, environmental, and regulatory developments result in a risk landscape that is changing ever more rapidly. These changes give rise to so-called emerging risks – newly developing or changing risks that are difficult to quantify and whose potential business impact is not yet, or only partly, taken into account at present. In addition to new risks emerging, growing interdependencies among known risks also can contribute to an increasing accumulation of risk and create substantial, unexpected ripple effects.

Risk perception survey

To improve understanding of the changing risk landscape, a risk perception survey targeting the company's employees was developed to identify and assess emerging risks. The survey accomplishes this through the systematic gathering of new risk *notions* (early/faint risk signals) and filtering them in an efficient and effective manner. The survey's results are used to aid in (1) enhancing risk dialogue, (2) reducing unexpected risk exposures, and (3) enabling new business.

This survey spans the entire risk classification system and supports risk identification across all risk categories, including property and casualty, life and health insurance risks; financial risks, and operational risks. In the past this was done by e-mail risk surveys and workshops; however, the survey was recently expanded to an interactive web-based platform with discussion groups.

Every employee has access to the platform with a growing number of staff from various countries actively signed up. Per year, more than 250 new risk entries from internal and external sources are added, of which roughly 10 percent prompt further formal study. Examples of notions include aspects of climate change and pandemics that were identified years ago when the survey was launched to more recent entries of cyber and power

blackout risks.

A roundtable is formed to analyze the risk perception survey, composed of both senior risk managers and senior business practitioners who are jointly in charge of filtering the risk notions, understanding how this might impact the insurance business, and coming up with the most relevant risks, along with concrete recommendations for senior management.

Emerging Risk Scenario Analysis

Although risks today are still assessed largely reactively based on loss experience, a faster pace of change requires a more anticipatory approach. This requires translating risks associated with high uncertainty into actionable measures based on early/faint signals – not on exact facts and figures – that can facilitate mitigating actions. Therefore, as part of emerging risk analysis, the notions tagged for further study often are subject to scenario development. Since scenarios are thought experiments about possible future states of the world, they are particularly useful to think proactively about potential risk impacts that involve a high degree of uncertainty, such as the notions generated in the survey. The results of the scenario analysis provide further decision-making support for senior management, and scenario losses can be added to the risk models, where deemed appropriate.

Key Lessons:

This ongoing Web 2.0 employee risk survey is effective in continuously gathering risk information from across the company and providing consolidated risk information to senior management from both risk management and the business units. Good steps have been taken over the past years on both emerging risk reporting and integrating emerging risk management into the company's overall risk control framework.

Work on the survey has clearly identified that historical risk data based on loss experience have to be complemented with current and future scenarios to manage risk uncertainty. To tackle the significant variation in risk perceptions, it is relevant to involve in such risk perception surveys, business experts from different educational and cultural backgrounds, as well as with varied business experience and from different geographic regions.

Further integrating the findings into standard risk management (e.g., risk committees, executive committee, board reporting) and business processes, as well as into strategy development is still work in progress. This involves assigning clear responsibility for new risk exposures and developing and implementing adequate mitigation measures.

EXAMPLE 8. INTEGRATING RISK INTO THE PLANNING CYCLE

The problem that needed to be addressed:

As the complexity of organizations and the environment in which they operate increases, firms need effective methods to systematically identify and assess the key risks to their strategy and develop and implement responses to these, while remaining within their desired risk appetite. Such methods need to be owned by senior management, embedded in the Enterprise Risk Management (ERM) framework, and linked to the day-to-day management of the firm.

How this firm went about addressing it:

For many years, this insurance firm had successfully helped large corporations improve their risk profile. Specialists were engaged to assess specific types of risks and identify potential mitigation actions to be implemented. During a period of significant change (late 1990s) the firm's leadership decided to adopt a similar methodology for assessing its own business and strategic risks and created the holistic process of Total Risk ProfilingTM (TRP).

To meet this objective the firm took a number of steps:

- Based on its experience and the expertise it had gained from serving its clients, the firm developed a group-wide standard to identify, assess, manage, and monitor risks that threatened the firm's ability to reach its strategic objectives and achieve its plans. The methodology was designed to help senior management take calculated risks more effectively and help define the risks a management team was prepared to accept and the risks they would not be willing to accept without further risk management action.
- The focus was widened from a narrow set of specific risks to apply to a wide range of business and strategic risks.
- Standardized implementation throughout the firm ensures a consistent global approach from the Board level to individual business units.
- To make this approach useful for managers, the process was aligned and linked with the business planning process at the time senior managers review risks to their business plan. The methodology requires managers to identify and then evaluate the probability of a risk scenario occurring, as well as the severity of the consequences should it occur. Risks that could impact the three-year rolling strategic plan are considered, and actions to mitigate these are identified and defined.
- The main focus is to embed mitigating actions into

operational plans and ensure senior management accountability for dealing with the risks identified.

- Progress against the defined actions is reviewed by management on an ongoing basis and reported up through the firm, thereby ensuring a transparent view of the development of the firm's risk profile and risk landscape.
- Alignment to management's planning processes, also means that the formal risk assessment is performed on a regular, periodic basis thereby supporting an up to date view of the underlying risk landscape.
- The risk assessment is embedded in the overall management processes and the methodology is also used to assess and mitigate risks in key change initiatives.
- The methodical, firm-wide approach supports the identification and coordinated response to more systematic risks; these are risks that may be pervasive across the firm and that require coordinated action driven from the center and guided by senior management to ensure that they are within the firm's desired risk appetite.
- Senior management's perspective on the risk profile is assisted by risk insights from the global risk function.

Key Lessons:

- Senior management sponsorship was key to implementing the process. For successful maintenance, sustained levels of senior management commitment and ongoing ownership, as well as consistent tone from the top are required.
- A single, global approach, readily understood throughout the organization, is key to embedding the ERM framework. This allows for a consistent perspective on risk appetite and a corresponding consistent approach to risk identification, assessment, and mitigation.
- Communication of management's risk appetite and cascading information on key risks to a global audience in a consistent manner is an essential component of the process.
- Embedding the assessment and mitigation actions into the planning and operational cycles ensures that the assessment is meaningful for senior management, rather than simply being a static and, for the most part, stand-alone process.
- After more than a decade of experience in applying this approach, critical success criteria for the future include maintaining its relevance by linking the process to the organizational structure and plan, providing management with both top-down and bottom-up risk

insights, and ensuring the review of strategic initiatives.

- The main implementation challenges to embedding this approach include; ensuring standard global implementation supported by education and training, developing and maintaining quality criteria, and providing easy-to-use tools and templates for the business community.

EXAMPLE 9. RISK APPETITE

The problem that needed to be addressed:

Post financial crisis, an increasing number of firms have fully or partially implemented risk appetite frameworks within their organizations. Despite the commitment made and effort expended, progress in implementing risk appetite frameworks has not always yielded the desired benefit of strengthening organizational risk culture. In some cases, firms have achieved buy-in to the concept but are struggling with its articulation and implementation.

How this firm went about addressing it:

Board and Senior Management Engagement

A high-level statement of risk appetite is discussed and approved at the Board risk committee level each year. This statement provides a concise view of the key quantitative and qualitative factors in overall risk appetite, is tracked regularly against quantitative metrics whenever possible, and has been communicated within the risk organization. The enterprise risk appetite statement has been cascaded to more granular risk appetite statements and similar metrics at the business line level.

Communication Strategy and Enterprise-Level Implementation

The broader communication throughout the enterprise has required some additional work to distill the statement into a shortened form suitable for a wide audience. The detailed enterprise risk appetite statement was distilled into five core risk management principles – succinctly summarized into five statements totaling twenty words – that would have meaning for all employees regardless of seniority or job function. These five principles have been embedded in education, on-boarding, and communications initiatives throughout the organization.

Link to Compensation and Performance Management

The overall quantitative and qualitative statements have been used to provide guidance on the operational risk appetite for the organization as well as guide the development of a scorecard integrated into the firm's incentive compensation structures, both in the design of new programs and in annual adjustments to compensation plans.

Ensuring that Risk Appetite Provides Actionable Guidance for the Business

Risk appetite provides actionable guidance when it is integrated into: 1) target setting of financial performance metrics; 2) business group strategy, both to reflect the current risk tolerance and its effect with the business strategy; and 3) the enterprise-level strategy process that defines the tolerances. This involves an interaction between senior management and the Board.

Key Lessons:

Benefits of a Robust Risk Appetite Framework

The key benefits from the implementation of the risk appetite have been as follows:

- The risk appetite acts as a statement of fundamental values for the organization, providing valuable direction in all risk-related decision making.
- Risk appetite engages the Board and regulators in a discussion on the appetite for risk taking.
- The cultural benefit of aligning all levels of the organization to approach decision making with the risk appetite framework in mind.

Implementation Challenges

Clarity: Significant time was required to first define the elements, get clarity from a diverse set of stakeholders, and achieve concurrence on the tolerance levels for quantitative metrics. The qualitative statement also represented a significant challenge, as these statements summarize and reflect business practices, philosophy, and culture. Consensus building at the Managing Board level was essential.

Relevance: Making the statements relevant to each line of business was a challenge; first in ensuring people understand why the metric is being used, and then in determining the tolerance appropriate for the business. The enterprise-wide risk appetite statement is being cascaded to metrics specific to each line of business to facilitate broader understanding and application. Additional work was necessary to distill the full statement into a short form suitable for a wide audience for communication throughout the organization.

Aggregation: Given that each line of business has customized the qualitative/quantitative statements based on its respective strategy, aggregation from strategy documents continues to be a challenge to determine if a business group is operating with acceptable levels. This does not impact the tracking of enterprise-wide defined metrics, but does suggest that there may be room for improvement in cascading from the enterprise view to the

line-of-business view. Another challenge was achieving sufficient clarity around the concept of risk appetite and some of the terminology used (e.g., difference between risk appetite and risk limits).

Key Success Factors

- Senior management engagement on the topic and their willingness to challenge their peers on the definitions and interpretation.
- Facilitating work sessions, not only with senior leaders, but also with mid-level management to ensure that items are relevant.

EXAMPLE 10. FORMALLY FACTORING RISK INTO RESOURCE AND BUDGET PLANNING

The problem that needed to be addressed:

A bank believed that to achieve sensible risk/return management, efficient resource allocation (particularly of capital and liquidity), and effective execution, a comprehensive resource and budget planning framework had to be implemented. In addition, the existing performance management system had to be enhanced to include a stronger and overarching risk view.

How one firm went about addressing this:

- An Enterprise Risk Management (ERM) framework with clear ownership model has been established with key elements, including:
 - Portfolio and risk analytics, particularly stress testing framework.
 - Capital adequacy management, including risk-bearing capacity calculation.
 - Risk management, including risk planning and budgeting.
- A Holding Steering Group (HSG) was established, consisting of the group's relevant management functions: Group Strategic Risk Management, Group Performance Management (GPM), Group Asset Liability Management (ALM) and Group Accounting.
- The logical sequence of tasks of the complex and comprehensive ERM framework (e.g., risk materiality assessment, stress tests) was integrated into a combined GPM/ERM process.
- Key deliverables, such as the group budget and risk appetite statement, are now derived from this integrated and iterative process

Key Lessons:

- The implementation of the HSG was a vital step to establishing a regular, weekly dialogue between all functions responsible for group management.
- Early discussion of relevant issues, methods, and strategies has led to increased efficiency and effectiveness and, more important acceptance and buy-in.
- The combined ERM/GPM process has led to comprehensive and more focused management.
- Single results, for example, from stress tests, are directly and immediately considered and translated into overall management action.

EXAMPLE 11. EMBEDDING RISK APPETITE IN THE ORGANIZATION

The problem that needed to be addressed:

Many firms have made progress in setting new risk appetite statements post crisis, but by and large risk appetite is not yet embedded in business decisions. This is in part because sometimes statements are not written with embedding as the end in mind. Looking at the metrics through this lens is important.

How one firm went about addressing this:

Calculation of risk capacity – firms are starting to consider risk capacity as the first step. This is the amount of risk that a bank can take and still remain viable in the face of adverse developments – i.e., that the potential losses or liquidity stresses faced by the bank would not undermine it. It sets the outer limit for risk appetite.

Metric selection for risk appetite – it contributes to the success of the projects to define and agree at the outset which core metrics will enable allocation. Another aspect of metric selection is the choice of the number of metrics. Having a sizeable number of different metrics can make embedding difficult and also can lead to conflict between different metrics.

Metric structure – the use of one core metric that can provide a common language across risk types and business units helps embedding. Likewise, being clear what constitutes a primary appetite metric and a monitoring metric helps the framework and its usability.

Core metrics:

- Ideally, at least one core metric should be applicable across all risk types and across all business units

Supporting metrics:

- Supporting metrics can then be added to complete the appetite for a business unit.

Monitoring metrics:

- It is important to have monitoring metrics to assess if business and strategy are still within risk appetite.

Linking the appetite to the limits

Thinking through the links between risk appetite and limits is also key. For some firms, limits are seen as the expression of risk appetite, but they are actually one of the methods of ensuring that appetite is met.

Key Lessons:

- Obtain the support of the CEO and involve both the risk and finance teams to achieve a successful risk appetite project.
- Consider the risk capacity and identify the underlying risk factors in the portfolios that could cause failure.
- Set clear goals for the risk appetite project and embedding of the appetite in the firm's culture.
- Spend sufficient time identifying, challenging, and aligning the metrics and set principles for governing the metrics.
- Structure and categorize metrics according to the core, supporting, and monitoring criteria
- Agile stress testing is critical to successfully embedding a risk appetite; lengthy delays in running traditional linear stress tests is a significant barrier to integrating risk into the annual planning cycle and equally supporting off-cycle risk challenges.
- Educate the Board on its role and the mechanics of the framework. Risk appetite should lead to the Board and the business to make hard decisions that may curtail some business decisions. It is crucial that the Board is aware of the objectives, the workings, and the implications of the risk appetite framework.

EXAMPLE 12. RISK AGGREGATION

The problem that needed to be addressed:

The bank primarily uses risk aggregation models to determine whether or not its actual risk profile is in line with its high-level risk appetite statements. To this end, developments in financial markets, regulatory changes, etc., are continuously reviewed, as rapid developments in these areas impact the applicability of risk aggregation approaches.

Furthermore, the lessons learned from previous crises are taken into account. This, for example, led to the redesign of the risk appetite framework in 2009, which was improved in a number of ways, such as:

- Making a better link between the risk metrics used and the key solvency ratios.
- Achieving better incorporation of accounting practices in calculations.
- Incorporating as a starting point the assumption that if the firm is in need of capital, it cannot be raised in the market, which means that earnings generation, and hence the capacity to restore capital should have a more prominent place in the risk appetite statement.

How this firm went about addressing it:

Currently, the solvency-related risk appetite statement is defined such that, in a 1-in-10-year event, the following should be adhered to:

1. The Core Tier 1 ratio (phased-in Basel III) remains above [x]percent and returns to the target level [y] percent after two years (through retained earnings).
2. The Basel III leverage ratio remains below [a] and returns to [b] after two years
3. The Core Tier 1 statement (1.) should also hold if regulatory capital is replaced by economic capital.

To verify that the actual risk profile is in line with the risk appetite statements, several risk metrics are calculated at the bank level. In particular, the following risk metrics are calculated:

- Earnings-at-risk: profit-and-loss impact for a 1-in-10-year scenario – Value at Risk (VaR) for the trading book is part of this calculation.
- Revaluation-reserves-at-risk: revaluation reserves-at-risk for a 1-in-10-year scenario.
- Risk weighted assets at-risk: RWA increase in 1-in-10-year scenario, in particular accounting for credit migration.
- Economic capital

For example, to be able to calculate the Core Tier 1 ratio in 1-in-10-year scenario, both Core Tier 1 capital and RWA need to be calculated in a 1-in-10-year scenario. Capital is influenced by P&L, covered by earnings-at-risk in the 1-in-10-year scenario, and revaluation reserves under Basel III, covered by revaluation reserves-at-risk. To determine RWA in a 1-in-10-year scenario RWA-at-risk is needed.

All metrics previously mentioned should incorporate the impact of a number of different risk types. For example, earnings-at-risk should contain the following elements:

- Credit risk costs and impairments.
- Negative impact on the interest margin of adverse interest rate movements.
- Equity impairments due to decreasing stock prices.
- Negative impact of operational risk related incidents (e.g., frauds, system failures, etc.).

As the elements mentioned are all calculated separately, and as the total potential impact of all these factors combined is required to calculate overall P&L impact in a 1-in-10-year scenario as well as the consequent impact on capital and solvency ratios, models are needed to aggregate the individual risks.

Key Lessons:

These models are based on either the Monte Carlo simulation or the variance-covariance method. The most important ingredient for these risk aggregation models are the correlations between the various risk types. The quality of the outcome is highly dependent on the accuracy of the correlations used, and therefore a lot of effort has been put into determining these. Sources used to substantiate the correlations include historical data analysis, position data analysis, external benchmarks, and expert opinions.

Furthermore, the principle used is that if there is uncertainty about the correlation (e.g., because the correlation cannot be substantiated by historical and/or position data), judgment is applied and the correlation is set conservatively.

EXAMPLE 13. LINKING RISK APPETITE TO RISK CONTROLS

The problem that needed to be addressed:

To operationalize its risk appetite, one insurance company has worked to strengthen the interface between the group's risk policy, which includes its risk tolerance, and group planning, and the risk taking activities and their corresponding risk controls at all levels of the group. This has required defining the group risk tolerance in a way that influences the business decisions, employing the risk tolerance to constrain risk appetite setting in the planning process and setting the group's risk limits consistent with both.

How this firm went about addressing it:

Group Risk Policy and the Risk Tolerance

Risk appetite setting starts with the Board of Directors establishing the group's risk policy. The operational element of the group risk policy is the group's risk tolerance. There are two critical considerations when defining the risk tolerance.

- First, the group should be adequately capitalized from a *respectability* perspective, that is, it should hold sufficient capital so as to be an attractive counterparty. This includes satisfying any relevant regulatory requirements.
- Second, the group should have adequate financial resources from a *franchise protection* perspective, that is, it should have sufficient capital and liquidity to be able to continue operations after an extreme loss.

The Board sets the criteria, and executive management translates the criteria into explicit capital and liquidity adequacy targets for the group and the major business units, and monitors the actual position against these targets on a monthly basis.

Group Risk Appetite

Within the boundaries imposed by the risk tolerance, the risk appetite is determined via the group's planning processes. For each planning run, several potential macroeconomic scenarios – including a baseline scenario and stress scenarios – are tested against the risk tolerance over all planning periods. For the baseline scenario, the Board expects the plan to be in compliance for all risk tolerance criteria over all planning periods. For the stress scenarios, the Executive Committee reviews any projected risk tolerance breaches and decides if any additional monitoring, limits or proactive defensive actions need to be incorporated into the plan.

Risk Limit Setting

Limits are established for major risk category and risk factors, and these are intended to supplement the high-level monitoring of risk tolerance with an added set of controls on the accumulation of risk exposure over the course of the year. These limits are sized according to the base scenario of the plan with an additional operational buffer added to each limit.

The full usage of all limits set at the group level is checked against the risk tolerance criteria. The top-level risk tolerance criteria for the group are expected to be met even under full limit usage. The lower-level, more granular limits at the business unit level can be in excess of risk tolerance under full limit usage.

Limit usage is monitored by the Executive Committee on a monthly basis. Any breaches of the limits at any level prompts an immediate limit review. During this review, limits may be resized by adjusting the buffers or adjusting the plan's overall assumptions, if necessary.

Key Lessons:

By defining the overall risk tolerance of the group using objective, measurable criteria, the group is able to develop risk tolerance targets that can both guide risk appetite setting in the plan and serve as the basis for the major risk limits of the group.

Going forward, the group faces two key challenges in setting its risk appetite:

- First, since the risk appetite is set through the planning process and limits are sized as a result, the flexibility and efficiency of this process has a direct impact on the ability to incorporate forward-looking analysis into the risk control framework. For this reason, time is spent continuously improving the efficiency of the planning process.
- Second, there is a constant dialogue with regional stakeholders, especially local regulators looking for assurance that the group-wide risk control framework and risk appetite provide sufficient controls to meet their concerns. Thus, there is a growing imperative to demonstrate how the group's controls support the solvency requirements of legal entities without reducing the value provided by the group's diversified capital base.

SECTION 3. ROLE OF THE BOARD AND BOARD RISK COMMITTEES

EXAMPLE 14. IMPLICATIONS OF TWO-TIER BOARD STRUCTURE FOR RISK COMMITTEES

The problem that needed to be addressed:

The specific corporate governance structure of a financial institution has consequences for the different committees that deal with risk issues. This includes membership, meeting frequency, mandates, and tasks and responsibilities. A typical two-tier board structure consists of a Supervisory Board (SB) and an Executive Board (EB). Both play an important role in managing and monitoring the risk management framework.

How one firm went about addressing this:

Executive Board

The EB is responsible for managing risks associated with the company's activities. Its responsibilities include ensuring that internal risk management and control systems are effective and that the company complies with relevant legislation and regulations. The EB reports on these issues and discusses the internal risk management and control systems with the SB.

At this bank the EB is supported by several committees that deal with specific risk topics. These committees act within the overall risk policy and delegated authorities granted by the EB and have an advisory role to the CRO. Another important governance element of the risk committees is that the chairman of each committee is responsible for making decisions, with advice from other committee members. Each committee is chaired by a senior risk representative.

Supervisory Board

The SB is responsible for supervising the policy of the EB, the general affairs of the company and its business, including financial policies and corporate structure. The SB has several subcommittees related to specific topics. The Risk Committee (RC) assists the SB on matters related to risk governance, risk policies, and risk appetite setting; it reports in the SB on the main risk issues in the company. Based on advice by the RC, the SB annually approves the Risk Appetite Statement for all financial and nonfinancial risks. On a quarterly basis, the EB reports on the company's risk profile versus its risk appetite to the RC, explaining changes in the risk profile.

The composition of the RC is determined based on relevant business know-how and adequate understanding of risk management-related issues. The RC comprises at least three members, who are member of the SB only. In addition, the meetings are attended by the chairs of the Audit Committee of the SB, the chair and vice-chair of the EB, the CRO, CFO, and the internal and external auditors.

The CRO attends RC meetings. The CRO ensures that the RC is well informed and understands the company's risk position at all times. Every quarter, the CRO reports to the RC on the company's risk appetite levels and on its risk profile. In addition, the CRO briefs the committee on developments in internal and external risk-related issues.

Key Lessons

- With the establishment of the RC, the discussions at SB level of the company on risk issues have gained depth. Whereas the Audit Committee predominantly focuses on actual results, the RC takes a more forward-looking approach.
 - The RC strengthens the annual process of determining the Risk Appetite Statement and linking it to the planning process.
 - Ongoing developments, from the perspective of the CRO, include finding a balance between bringing quantitative and qualitative information to the RC, and between the level of aggregation of risk information and detailed information on business unit level.
 - In the area of nonfinancial risks, it remains a challenge to determine the level of information to be submitted to the RC, as aggregation of these risks is per definition difficult.
- The bank created a risk committee at the Executive Management level in 2008, as a lesson learned from the crisis. Its main objective is to discuss the bank's risk appetite, current risks, trends, and concerns.
 - Participants: Subgroup of Group Executive Committee, that is, the CEO, CRO, CFO, heads of business segments (investment bank, domestic and international retail bank, and asset management).
 - More precisely, the risk committee's mission covers the following topics:
 - Defines the risk appetite by acting as a validation forum for new risk appetite policies, such as the risk appetite statement and concentration policies.
 - Reviews decisions taken in other committees, such as counterparty level or portfolio level committees, during the month.
 - Facilitates discussions related to current events and risk areas.
 - Identifies topics/issues to be analyzed and subject to decision making in operational committees (Risk Policy Committee or Capital Market Policy).
 - Makes decisions on organizational topics.
 - The risk committee at the Executive Management level illustrates the strong involvement of Executive Management in making risk and risk appetite a driver of strategic and business decisions.

EXAMPLE 15. HOW A RISK COMMITTEE HAS BEEN EFFECTIVELY STRENGTHENED

The problem that needed to be addressed:

It is commonly agreed that increased Board engagement in risk management is essential to strengthening risk governance. This also is dependent on having effective risk reporting to the Board, striking the balance between providing enough information without having the Board get lost in the details.

How this firm went about addressing it:

Risk Committee at the Executive Management Level (Board in its Executive function)

- The risk committee at the Executive Management level illustrates the strong involvement of Executive Management in making risk and risk appetite a driver of strategic and business decisions.

Risk Committee at Board Level (Board in its Supervisory function)

- The risk function reports regularly to the Internal Control, Risk, and Compliance Committee of the Board on its main findings, as well as on the methods used by the risk function to measure these risks and consolidate them on a group-wide basis

- These committees at the Board level meet quarterly and consider the group's risk management in accordance with applicable regulations, as well as reviewing specific issues and methodologies.
- More precisely, the committee reviews changes in market, counterparty, and credit risks as follows:
 - Capital market topics and value-at-risk (VaR) trends, as well as the results of the stress tests carried out on market risk.
 - Credit risks evolution in the retail/corporate businesses, geographical and industry portfolio distribution and concentrations, the main exposures, and watchlists.
 - The conclusions of the Risk Policy Committees as well as Strategic Countries Reviews.
 - All other matters related to methodologies, additional stress test results, or any other hot spots.

The Links Between These Two Risk Committees

- Executive Management regularly presents its risk appetite for review to the Board.

Key Lessons:

The risk dialogue with the Board has been in place for some time and has intensified with the recent financial crisis. Reports to the Board include better explanations, simpler terms, and more-detailed risk information. This helped facilitate a better understanding of risk by the Board, as well as promoting more interactions on the topic.

Areas of improvement are to further integrate the risk, capital, and liquidity analysis provided to the Board, as well as continuing to enhance reporting on an ongoing basis.

EXAMPLE 16. INTERACTION OF THE RISK COMMITTEE WITH OTHER BOARD COMMITTEES

The problem that needed to be addressed:

Ensuring that risk considerations are appropriately taken into account in Board committee discussions and that risk strategy is appropriately linked at the Board level.

How this firm went about addressing it:

The Board of Directors is ultimately responsible for and therefore has an essential oversight role, in risk management. The Board Risk Committee has the mandate of supporting the Board in performing its responsibilities related to risk and capital management and alignment with strategy. To be effective, the Risk Committee must interact appropriately with other Board committees, in particular the Audit, Remuneration, and Strategy Committees.

First, the bank defined the membership of Board committees to ensure appropriate synergy and effective interactions between the Risk Committee and the other relevant committees:

- The chairman of the Risk Committee has a seat on the Remuneration Committee, which has the mandate to promote and encourage discussions on compensation; discuss and analyze the existing models of compensation, taking into account market practices; and adjusting the compensation models to ensure alignment with the bank's risk management and control objectives.
- The chairman of the Audit Committee also has a seat on the Risk Committee. The Audit Committee is the body responsible for supervising internal controls and risk controls, as well as internal and external audit activities. In this capacity, it receives information not only from the risk function, but also from internal audit, which has a direct reporting line to the Chairman of the Board. Also, in accordance with the bank's risk appetite governance procedures, the Audit Committee receives quarterly updates on the progress of risk appetite implementation, with particular focus on the robustness of the processes and controls supporting the monitoring of risk appetite.
- Finally, the CEO is a member both of the Risk Committee and of the Strategy Committee, whose mandate is to support the Board in defining strategic and budgetary guidance for the group.

Therefore, there are Risk Committee members sitting on each of the Board committees with which the Risk Committee has significant points of interaction. This is extremely helpful in promoting information sharing and

coordination, as well as in ensuring that risk considerations are appropriately taken into account in strategy and remuneration discussions.

Second, the Board governance determines that all deliberations must be approved by the full Board, with Board committees responsible for examining options and recommending a course of action, but not for making final decisions. This arrangement helps ensure that decisions take into account all relevant aspects that might have been discussed in-depth in individual committees and that these are considered in making a final decision.

Finally, the necessary coordination of Board committee agendas required to support this governance process is greatly assisted by a very senior Board Secretary, who attends all Board committee meetings and is responsible for managing agendas and minutes. The Board Secretary plays a key role in connecting the dots between the multiple high-level discussions taking place in Board committees, and in making sure that information flows where needed and discussions evolve as required to reach the full Board at the right time.

Key Lessons:

The structural aspects of Board committee design, such as defining the mandates and the membership of Board committees in a way that facilitates interaction of the Risk Committee with the other committees is an important starting point. In particular, the presence of members of the Risk Committee on other relevant Board committees (e.g., Audit, Remuneration, and Strategy) is extremely helpful in ensuring that risk considerations are appropriately taken into account in the deliberations of other Board committees, as well as in ensuring effective linkage between risk and strategy at the Board level. Another important lesson is that effective interaction between Board committees is greatly facilitated by the presence of a senior Board Secretary with the mandate of managing Board processes to ensure, among other things, coordination and appropriate interaction among committees.

Current plans include strengthening the links between the Risk Committee and the Strategy Committee by increasing the involvement of the Risk Committee on risk assessment of mergers and acquisitions transactions, as well as involving the Strategy Committee in the annual risk appetite review process.

EXAMPLE 17. INTERACTION OF THE RISK COMMITTEE WITH OTHER BOARD COMMITTEES (E.G., AUDIT, CREDIT RISK, ETC.)

The problem that needed to be addressed:

The bank had already implemented a high-frequency reporting regime for quite some time, in which all risk portfolios across the globe were reviewed using a bank-wide standard suite of simple metrics allowing the firm to easily pick up on trends and behaviors .

It was, however deemed necessary to ensure that risk management and oversight responsibilities would not be restricted to, or encapsulated within, the boundaries of the risk committee of the Board; and that, on the contrary, it would spill over and permeate other relevant committees appointed by the Board. Equally, the firm wanted to ensure that relevant, albeit filtered, information would end up at the Board risk committee.

The overarching aim was that all critical aspects of management, be it finance, business development, remuneration, compliance, or reputation, would be fully aligned and that all relevant groups and committees would act upon the risk appetite set by the Board. Thus, the appropriate incentives would be in place to guarantee full alignment between risk appetite and other financial and business targets pursued by the management.

How the firm went about addressing it:

The firm's Board, which meets on a monthly basis, created the following Board committees:

Executive Committee

Composed of nine Board members, of which five are non-executive directors (NEDs); assumed all the powers of the Board that have been delegated to the Executive Committee, including the following:

- Approval of the general policies and strategies of the company: strategic plans, management targets and annual budget.
- Submission of decisions on dividend and treasury stock policy to the full Board.
- General risk management policy.
- Corporate governance policy.
- Corporate social responsibility policy.
- Control of management activities and evaluation of managers.

The Executive Committee meets on a weekly basis.

Board Risk Committee

Composed of five Board members of which three are NEDs, responsible for all risks affecting the institution: includes proposing the risk policy, including setting risk appetite and follow-up, information and internal control systems, mitigation plans, risk management tools and models (including their internal validation), and approving transactions up to a pre-determined level, with excess amounts referred to the Executive Committee, to the Board

- The Board risk committee meets twice a week.
- The chairman of the Bank and the CEO are not members of the risk committee. This ensures that setting of risk policy is fully independent from management.

Audit and Compliance Committee:

Composed of five Board members (all of them NEDs); responsible for proposing the appointment of the external auditor, ensuring its independence; oversees internal audit services and reports, the preparation of financial information, compliance, control, and systems

Appointments and Remuneration Committee:

Composed of five Board members (all of them NEDs). Responsibilities include proposing to the Board: the remuneration policy for senior management, individual compensation for directors; basic terms for senior management; and the remuneration of those officers who, while not members of senior management, receive significant compensation particularly variable compensation and whose activities may have a significant impact on the assumption of risk.

Other Board committees:

International Advisory Committee: Technology, Productivity, and Quality Committee

- To achieve the aforementioned objectives, emphasis was placed on cross-membership and on channeling information from risk and audit groups to the different Board committees. Further consistency is assured by having the General Counsel of the firm act as Secretary to the Board and all Board committees.

The high frequency of the meetings of the Board Risk Committee and of the Executive Committee ensures that the senior management and Board members, including the NEDs, are fully involved in setting the company's risk policy and following up on the risk profile. Moreover, the structure of cross-membership among these Board committees ensures that there is full alignment between setting and following up on risk appetite, risk policy, and risk management actions; compliance and audit issues and remuneration policy matters.

Furthermore, the integral Risk Department submits its reports to both the Board Risk Committee and to the Audit Committee. The aim is to report on the performance of the risk division against international best practices and regulatory guidance, requiring senior management to receive complete and timely information covering all risks and comparing the approved risk appetite against results. Reporting includes recommendations on risk management issued following any examinations by any supervisor.

Senior risk officers regularly attend the Board Risk Committee and the Executive Committee when presenting transactions, risk management frameworks, and risk policies for approval. In turn, these risk officers chair, or are members of, more junior risk committees. This arrangement allows the risk culture and tone from the top to be quickly disseminated throughout the whole organization. As a matter of principle, transaction approval needs to be endorsed by collegiate decisions within committees, the seniority of the committee depending on the characteristics of the transaction. No personal authorization capacity is granted to anybody, including the CEO.

Key Lessons:

Prudent risk management has traditionally been the cornerstone of the firm's management throughout its existence. In particular the very active involvement of senior management and Board members, including many NEDs, in risk management and oversight, and the cross-membership structure of the Board committees ensure that there is full alignment between setting of the risk appetite and follow-up, business goals, financial management and compensation policy.

EXAMPLE 18. RISK REPORTING

The problem that needed to be addressed:

One multinational firm identified the need to upgrade its risk management information systems (MIS) for the Board. The pre-existing risk MIS package had a number of limitations, including:

- Unstructured and overly detailed risk reports that were not conducive to meaningful discussion.
- Lack of focus on ex-ante risk issues and on actionable information, with too much focus on ex-post measurement.
- Variability in metrics used across different operating entities.
- No aggregated view on overall risk and a resulting weak link to the risk appetite statement.
- Limited contribution from nonrisk functions, such as the CFO and key business units.

How the firm went about addressing it:

Consequently, the risk function implemented two MIS structures. First, an intermediate reporting structure designed to meet "minimal" risk monitoring objectives was implemented within three months. The ultimate objective—a reporting structure delivering the required risk/return and decision-making focus—was implemented within one year.

Some of the key features of the intermediate solutions were a lean and modular structure, including a short summary of key messages. Use of the modular structure allowed different risk types, geographies, and businesses to be presented in a consistent format.

An action-oriented approach was taken to risk reporting for the Board. Contributors had an obligation to give their professional opinion on the potential implications for the firm of any risk issues reported. In addition, at the end of each section of the report (e.g., credit risk) a synthesis of the key implications and proposed decisions required was mandatory. This increased accountability for risk within the business unit producing the report. Monitoring at the Board level of implementation of decisions made as a result of risk reporting further reinforced accountability.

A minimum set of common and consistent Key Performance Indicators (KPIs) was defined based on the availability of data across countries, the level of confidence in data quality, and the availability of timely information (e.g., at least monthly or quarterly). The time and resources needed for measurement and preparation of the reports was also a factor in defining the KPIs.

Consistency of the metrics used with risk appetite definitions was important, and simplified risk aggregation

metrics were defined to ensure a link with the risk appetite definitions used, including:

- Loss absorption capacity and Risk Adjusted Return on Capital (RAROC) and for P&L risk.
- Solvency and liquidity ratios for regulatory risk.
- Expected loss vs. impairments and Non Performing Loans (NPL) ratios for credit risk.

Available stress scenarios to ensure proper measurement of usage of tolerance levels also were incorporated.

Additional features implemented in the long-term, permanent risk reporting program included:

- Implementing metrics for reporting of nonprudential risks, such as reputational, legal, compliance, and audit risk.
- Incorporating reporting with a "house-view" on key macro-economic and sociopolitical trends to ensure a common understanding of the external context in which key risk implications for the firm were derived.
- Taking a forward-looking perspective and integrating risk reporting into strategic planning, in addition to reporting incorporated P&L and balance sheet sensitivity analysis to different risk types.
- Utilizing additional contributions from the CFO and the business units to better assess the implications of and make recommendations to the Board on risk issues. For example, the head of Capital Management might provide a recommendation on solvency issues highlighted in the report.
- Developing a group-wide risk data warehouse to progressively improve the consistency and quality of information across all risk types.

Key Lessons:

The risk reporting MIS upgrade was coordinated with the firm's broader risk culture program to ensure full alignment of the risk concepts and metrics used. Initial discussions included the involvement of Board members to ensure that the risk reporting package developed complemented the firm's risk governance structure. This integration of risk reporting with the firm's strategy and governance structure, and the explicit incorporation of macro factors, assisted the Board in using risk reporting to inform high-level, forward-looking decision making.

EXAMPLE 19. A MANAGEMENT INFORMATION SYSTEM (MIS) PACK THAT ALLOWS BOARDS TO ASSESS RISK EFFECTIVELY

The problem that needed to be addressed:

Boards require relevant, timely, and insightful information about the risk exposures of the firm in an easily understandable format, which covers all key risks and highlights key exposures to emerging risks.

How the firm went about addressing it:

This insurance company developed a risk management dashboard that is shared with a Risk Committee of the Board. While this committee is responsible for overseeing the assessment and management of material risks in the firm, it relies on other committees, such as the Audit and Investments Committees to oversee certain aspects of risk.

To ensure that the Risk Committee is informed of the status of all material risks in the firm, the dashboard is comprehensive covering credit risk, market risk, insurance risk, operational risk, liquidity risk, and capital adequacy measures. The dashboard, which is presented in PowerPoint form, starts with an executive summary highlighting movements in key risk exposures by risk type and summarizing other insights from the report.

For market risk, the portfolio mix is shown, by type of asset and, separately, by credit quality. In both cases, comparisons to prior periods are provided. In addition, trends are shown in economic capital usage by asset class as well as showing how each asset class compares to the economic capital and book value limit structures established and approved by the Investment Committee of the Board. Finally, realized and unrealized investment gains and losses are tracked and compared to prior periods.

The key market risk for the firm is interest rate risk. Therefore, in the risk dashboard, the focus is on asset liability matching. Assets are compared to portfolio targets, and liabilities and mismatches are measured and reported. In addition, the company has recently established an aggregate economic capital based-market risk guideline covering interest rate, equity, and currency risks, which will be reported going forward. Currency exposures also are reported against specific approved guidelines established by the management risk committee.

For insurance risks, trends in mortality, morbidity, and property and casualty loss experience (with and without the effects of catastrophes) are reported through the use of actual to expected benefit ratios. Operational risk events, many of which are reported to the Audit Committee, are summarized for those events exceeding a minimum

threshold.

Available liquidity is reported at several intervals up to one year, based on the results of the company's liquidity stress test for the most recent and three prior periods. Capital adequacy measures are reported and compared to company targets for various regulatory ratios as well as the company's overall economic capital solvency confidence target. Finally, the dashboard includes the overall results of the company's quarterly stress tests and its qualitative assessment of capital.

The executive summary and the details in the dashboard have been valuable to the Board to get a snapshot of the company's risk positions and trends. It also provides the opportunity to explore issues with management or independently with the CRO in executive session at the Board meeting.

With a recent change to the corporate organizational structure, the firm will be setting limits at the regional level and adding summaries of regional limits to the dashboard. Countries within regions are expected to produce similar dashboards as part of the organization's overall risk governance process.

EXAMPLE 20. ROLE OF BOARD IN STRESS TESTING

The problem that needed to be addressed:

Implement a group-wide stress testing process that involves senior management and the Board. The process should form part of business as usual strategic planning processes and involve the Board throughout.

How this firm went about addressing it:

- Stress testing is embedded within the organization and forms an integral part of the bank group's risk management framework and strategic planning processes.
- Stress testing scenarios are developed as part of the strategic planning processes and are presented to the Board for approval prior to their being utilized as part of the bank's planning processes. The rationale for particular scenarios and their anticipated impact (the "story line" behind the scenarios) are explained and documented so that the Board and senior management are aware of the stress testing being performed.
- Macro-economic stress testing entails four scenarios 1) positive scenario as compared to the budget; 2) budget scenario; 3) mild recession scenario; and 4) deep recession scenario.
- Once the scenarios are developed and approved by the Board, economic indicators for the scenarios are developed, which are then presented to the Board for approval.
- Detailed economic assumptions are mapped to the scenarios reflecting the types of risks and assets across the business. The scenarios considered incorporate changes in macro-economic variables, which include gross domestic product, employment levels, inflation and interest rates, equity prices, and property prices;
- The stress tests simulate the statement of financial position and profit-and-loss effects of stresses across the group, analyzing the impact on profits and the ability to maintain appropriate capital ratios and liquidity levels.
- Management considers applicable management actions as part of the stress testing processes and is required to review the implementation of management actions and quantify its impact.
- The business results and management actions are reviewed and challenged by the risk managers and senior management and by Group Risk as part of the detailed review meetings.
- Results are reviewed and approved by the Board Risk

Committee and ultimately by the Board

- Stress testing results are presented to the Board simultaneously with their risk appetite proposals and the capital plan to allow the Board risk committee and the Board to evaluate the proposed risk appetite and capital plan compared to the stress testing outputs. This is done as part of the annual budgeting process.
- On an ongoing basis, the group tracks a number of economic indicators against trigger levels, as identified during the stress testing process, as 'early warning indicators and to provide context for a forward-looking discussion at the Board risk committee.

Key Lessons:

- Stress testing should be part of the strategic planning processes, including the short- and long-term budgeting process and interaction with the Board should form part of the strategy and budget processes
- The Board should be involved throughout the process, including during development of the storyline behind the scenarios and the resultant economic indicators, and not just presented with the final results
- Stress testing results should show the impact on financial volatility risk appetite measures (e.g., ROE, Core Tier 1 capital ratio, loan loss rate) per scenario for discussion at the Board.
- Significant economic indicators identified during the stress testing process should be monitored against trigger levels to enable a regular forward-looking discussion by the Board risk committee.

EXAMPLE 21. ROLE OF BOARD IN STRESS TESTING

The problem that needed to be addressed:

Implementing a group-wide stress testing process that involves the bank's senior management and the Board. The main challenge was to develop the stress testing program in such a way that the technical complexity of risk models could be dealt with at a detailed level, but at the same time produce results that the Board can easily understand.

How this firm went about addressing it:

- A stress testing program was developed that specifically dealt with two components: 1) macro-economic stress and 2) event risk stress.
- Macro-economic stress testing entails four scenarios: 1) core house view; 2) downside risk scenario; 3) upside risk scenario; and 4) severe stress scenario.
- For event risk, various risk-type scenarios are defined by risk owners on a bottom-up basis mostly focused on tail risk of a large magnitude. Existing risk methodologies and quantification mechanisms are used to inform this process.
- Macro-economic scenarios are presented to senior management and the Board for discussion and approval prior to execution of stress testing.
- Once stress testing results are made available, they are then presented to various fora, including the Board for discussion and approval.
- Stress testing results are presented to articulate the past, present, and future earnings path for each of the four macro-economic scenarios. The macro-economic scenarios are then overlaid by the various event risk scenarios. Different permutations of event risk scenarios are used to illustrate interconnectedness and risk concentrations. In addition, capital adequacy stress testing results are also supplied as key output

Key Lessons:

- The Board normally has difficulty understanding complex aspects of stress test results, such as confidence intervals and quantitative assumptions. Even though 1-in-7 and 1-in-40 concepts are used in the risk type-specific measures, the results have purposely not been articulated in this manner, as it tends to create confusions as to the probability of the risk events. Instead, risk events have been presented by focusing on severity per macro scenario rather than by confidence intervals. Board members are able to obtain a much better understanding of stress testing results in this

way, as they were able to understand the scenarios and resulting impact on earnings and capital.

- Significant emphasis was placed on how stress testing impacts earnings volatility as earnings are seen as the first level of loss absorption. Loss of confidence tends to appear when earnings fall too much. Visual representation of earnings path with an event risk overlay proved to be very valuable to illustrate stress testing results on earnings volatility to the Board members.
- The annual Board risk assessment process also is used to further inform scenarios and test the understanding of Board members. Any lessons from this process, or gaps identified, are used to supplement stress testing either from an event-risk perspective or to highlight further areas of focus. The annual Board risk assessment is performed on a "blank sheet" basis to eliminate bias as much as possible, whereby Board members are asked on an individual basis to list key risks, comments, concerns, and any suggestions they may have.

EXAMPLE 22. BOARD SELF-EVALUATION RISK PROCESSES

The problem that needed to be addressed:

The problem was to ensure that a process/system of evaluation was designed that could be used to show that Boards, and Board committees, were functioning effectively and efficiently. It was recognized that an evaluation:

1. Should not (indeed, could not) be a tick-box exercise.
2. Needed to demonstrate to all stakeholders that in conducting a Board, or Board committee, self-evaluation, the directors and members of the Board and Board committees had, in so far as risk, governance, and compliance were concerned, met the requirements of:
 - Current regulations.
 - International best practice.
 - Board and Board committee charters.
3. Processes must be able to demonstrate that directors (and committee members) had discharged their fiduciary duties.

How the firm went about addressing it:

The bank recognized that any evaluation without a number of antecedent steps was of little value. The functioning of the Board and Board committees had to be consistent with the nature, the complexity, and all the risk and governance issues inherent in the activities of the business. A self-evaluation:

- Should be able to demonstrate that corporate behavior was universally recognized and accepted as correct and proper.
- Should show that the directors' conduct during the period was responsible.
- Could be used to show that directors and committee members had discharged their fiduciary duties with due regard for the nature and extent of the risks evaluated by the committee and the attendant governance issues.

The functioning of Board committees was premised on committees receiving appropriate direction from the Board in regard to the nature and extent of their responsibilities (see the following "antecedent requirements"), and on their reporting to the Board effectively and on an ongoing basis on the performance of the committee.

The antecedent requirements

To ensure that the evaluation was effective, a system has been embedded in the company that consists of a:

- *Charter* that sets out the roles and responsibilities of the committee in clear, unambiguous yet concise terms, including setting out the full nature and extent of the risk and governance issues for which the committee is responsible.
- A comprehensive *agenda matrix* that shows all the items needed to be dealt with during the year and their frequency. This document shows, on a quarterly basis, the time and the manner in which risks are to be dealt with by the committee.
- Clear *procedural guidelines* for the conduct of the proceedings of Board and Board committees
- *Continuous training* of directors and committee members on the business of Board committees by subject-matter experts.
- An enterprise-wide risk framework and *reporting system* that ensures the timely, accurate, and meaningful disclosure of matters material to the business of the company or the interests of the stakeholders. Directors and committee members receive timely and sufficient information, not data that enable them to focus on decision making and effectively make informed decisions.

Key Lessons:

It has been found that the only reliable method to conduct meaningful evaluations is to ensure that the correct foundational elements are in place, which consists of ensuring the antecedent requirements are all in place. In designing a Board self-evaluation system, it is important to ensure that the results show:

- Whether the Board, or Board committee, has:
 - Met the requirements of its charter and effectively dealt with the risks and governance issues it is required to consider.
 - Discharged its duties in terms of the applicable regulations setting out the risk universe within the committee's remit.
- If there is good communication between the Board and its committees, that is that committees receive appropriate direction from the Board and are aware of the nature and extent of their responsibilities.
- That committee meetings are productive, decisions are reached with appropriate actions allocated, and that all the items covered by the agenda were addressed.
- That the information received is appropriate and

sufficient to allow the Board or its committees to consider and make decisions on risk and governance issues.

A simple scoring system should be used to easily extract results. Overly elaborate scoring systems inevitably require substantial interpretation and can lead to fuzzy results that are not particularly useful. The principal challenges faced in conducting such an exercise is to ensure that an end-to-end process (i.e., all the antecedent requirements and evaluations) is in place. This involves a considerable amount of work, but it does have many advantages in assessing the efficiency and effectiveness of Boards and committees. Board and committee evaluations cannot be standardized or generic in nature. Given the vast range of risks that financial institutions face, a specific, tailor-made evaluation is necessary for each committee.

SECTION 4. ROLE OF THE CRO

EXAMPLE 23. DELEGATION OF RISK GOVERNANCE RESPONSIBILITIES

The problem that needed to be addressed:

To effectively discharge its fiduciary duties, the Board of Directors (the Board) must ensure the delegation of its risk oversight responsibilities is appropriate without compromising its primary goal of ensuring the firm's long-term success by delivering sustainable shareholder value within a framework of prudent and effective risk assessment and management.

How this firm went about addressing it:

The bank's Board explicitly delegated its risk oversight responsibilities to the risk committee, the Group CEO, and the Executive Board.

Committees

In 2008, the Board established the following committees to assist in the performance of its responsibilities:

- a) Audit Committee (AC)
- b) Corporate Responsibility Committee (CRC)
- c) Governance and Nominating Committee (GNC)
- d) Human Resources and Compensation Committee (CC)
- e) Risk Committee (RC)
- f) Strategy Committee (SC)

Each committee has a formal mandate and must be composed of non-executive Board members fulfilling strict independence criteria. The committee chairs are charged with ensuring that the Board is kept informed in a timely and appropriate manner of resolutions, decisions taken, activities, and issues. The committee structures and mandates are designed to complement each other, and joint sessions are regularly held, in particular, between the RC and AC and the RC and CC.

The function of the RC is to oversee and support the Board in fulfilling its duty to supervise and set appropriate risk management and control principles in for: (i) risk, including credit, market, and operational risks; (ii) treasury and capital management; and (iii) balance sheet management.

The RC responsibilities include:

- a) Proposing the guiding risk principles, including delegation of risk authorities and major risk limits, and recommending any changes required to these principles to the full Board.

b) Reviewing and approving the internal risk management and control framework across all relevant risk categories. This includes the roles and responsibilities of the Executive Board (EB), the regional and divisional CEOs, Group Chief Risk Officer, Group Financial Officer, Group Treasurer, and Group General Counsel.

Executive Delegation

The management of the firm is delegated to the EB under the leadership of the Group CEO.

The risk committee is not involved in the day-to-day management of risk, but it does look to the CEO and senior executive to demonstrate that they are fully engaged in the prudent management of risks. To support the RC in the discharge of the Board's risk oversight responsibilities, the EB is obligated to provide all relevant information to the RC.

The Group CEO, the Group CFO, and the Group CRO are responsible for assessing and managing the firm's risk and are ultimately accountable to the Board. Together, they have overall responsibility for establishing and supervising the implementation of the risk principles, for approving the core risk policies (as proposed by the Group CRO), and for controlling the risk profile of the firm as a whole.

The Group CEO is the highest executive officer of the firm and has responsibility and accountability for the management and performance of the firm.

Executive management, under the leadership of the Group CEO, are responsible for establishing an appropriate risk management environment, including a robust infrastructure and a strong risk culture, by aligning business planning, management, performance measurement, and compensation decisions with the firm's strategy.

Business management is responsible for making risk identification, assessment, measurement, and management critical components of their day-to-day business operations.

Risk Delegation

The Group Chief Risk Officer has explicit authorities and responsibilities and his/her appointment is proposed by the Group CEO and approved by the Board.

The Group CRO is responsible for the development and implementation of principles and the appropriate risk frameworks for credit, market and operational risks. The Group CRO assumes responsibility for the implementation of an independent risk function. The Group CRO approves transactions, positions, exposures, and provisions in accordance with the risk authorities delegated by the Board and set out in the firm's regulations.

Although reporting to the Group CEO, the Group CRO has an obligation to advise the chairman as well as the RC

on significant risk issues.

Internal Audit Delegation

Internal Audit's role, responsibilities, and authorities are set out in its charter, which is approved by the Board. The head of Internal Audit reports directly to the Chairman of the Board and to the RC. Internal Audit is fully independent of executive management, and its power to audit is unrestricted.

Internal Audit monitors compliance with legal and regulatory requirements and the organization's internal regulations and policies. It specifically verifies, or assesses, whether internal controls are commensurate with the risk and whether they are working effectively.

Key Lessons:

By providing explicit delegation of risk governance responsibilities and clear communication paths for escalating issues and concerns, the Board has ensured that the firm's executive management and risk function are completely clear about their duties and responsibilities to implement a robust and operationally effective risk framework.

Going forward, the firm faces the ongoing challenge of ensuring that individuals understand that although risk responsibility can be delegated, accountability cannot be abdicated. The accountability for appropriate supervision and oversight of delegated activities remains.

EXAMPLE 24. FORMAL STATEMENT OF OWNERSHIP OF RISK

The problem that needed to be addressed:

Who is responsible for the development and ownership of the risk framework, and who ultimately owns the risks?

How this firm went about addressing it:

- Main principles of risk ownership at this bank:
 - Business lines have primary responsibility for risk: The main responsibility for risk remains in the hands of the core businesses and the business lines originating risk. Accordingly, the responsibilities of the different participants must be clearly established and should be in line with the bank's internal control principles. The business lines need to facilitate an understanding of risk among their staff and remain aware of changes in the bank's exposure to risk.
 - The risk function contributes as a second level of control, reviewing transactions and new activities, to ensure that the credit and market risks taken by the firm comply with and are compatible with its policy, its desired credit rating and its profitability targets.
- Main principles of the risk function's organization:
 - Strong and independent supervision and control functions.
 - The risk function is headed by the CRO, who reports to the CEO and is a member of the Executive Committee.
 - The duties associated with the risk function at group risk management level are exercised independently of the divisions and support functions.
 - The CRO has the right of veto on risk decisions made by the group.
- Key responsibilities of the risk function are: identifying risk, anticipating risk trends, measuring risk, providing risk information, and contributing to risk decisions.
 - All risks resulting from the group's business operations are covered. The risk function intervenes at all levels in the risk taking and monitoring process and its remit includes formulating recommendations on risk policy, analyzing the loan portfolio on a forward-looking basis, approving corporate loans and trading limits, guaranteeing the quality and effectiveness of monitoring procedures, defining and/or validating risk measurement methods, and producing comprehensive and reliable risk reporting data for group management.
 - Risk also is responsible for ensuring that all the risk implications of new businesses or products have been adequately evaluated. The quality of the validation

process is overseen by the risk function, which reviews identified risks and the resources deployed to mitigate them, as well as defining the minimum criteria to be met to ensure that growth is based on sound business practices.

- It is the finance department that drives the budget and capital planning process, with risk contributing as a "second pair of eyes" on forecasts and budgets prepared by the business.
- Risk is involved in the definition of the principles of the firm's liquidity policy. As part of its second level's control function, risk validates models; risk indicators, including liquidity stress tests; limits; and parameters. Risk also participates in group's Asset Liability Management (ALM) committee.

Key Lessons:

The risk department is a global, fully integrated function. It is the primary instrument for the development, implementation, and transmission of the risk appetite, keeping in mind that a key principle is that the business lines have primary responsibility for risk. Hence, the importance of maintaining and developing a strong risk culture in order to promote a consistent risk approach throughout the group.

EXAMPLE 25. FORMAL STATEMENT OF OWNERSHIP OF RISK

The problem that needed to be addressed:

The Board of Directors (the Board) exercises ultimate supervision over the executive management of the firm, and therefore must ensure that individuals throughout the firm are clear on their accountabilities and responsibilities to prudently manage risk in a manner consistent with the firm's strategic priorities and values and within the firm's risk-taking capacity.

How this firm went about addressing it:

The bank established and published a formal statement to clearly set out accountability for risk taking, whether explicit or implicit, and the independent oversight of these activities.

The formal statement, known as the Risk Principles, is owned and approved by the Board.

The group CRO is explicitly responsible for the development and implementation of these Risk Principles, which require the establishment of effective risk frameworks for credit, market, and operational risks.

The Risk Principles explicitly require:

- The CEO *to be accountable* for all risks assumed within their division.
- The front office (or equivalent—revenue generating/client-facing unit) *to own* all risks taken within a division.
- The implementation of an independent risk function *to oversee* a division's risk taking activities.

The divisional CEO is accountable for ensuring that the front office continuously, actively, and appropriately balances the risks taken against the associated reward. The CEO must ensure that the division's risk profile remains within its risk appetite and is consistent with the division's strategy.

The independent risk function monitors the effectiveness of the management of the division's risk profile. The risk function provides an independent and objective check on the front office's risk-taking activities.

Key Lessons:

Underlying the Risk Principles is the tenet that risk decisions are made *ad-personam* and that before any risk can be assumed by the firm both business management (the front office) and the risk function must approve it within the risk authorities delegated to them by the Board. Front-office approval, whether explicit or implicit, denotes the

acceptance of full accountability for any losses incurred.

The risk officer's approval is seen as a positive statement that the risk is considered acceptable, both quantitatively and qualitatively, and that there is no reason to doubt the ability of the front office to manage the risk. It is expected that risk officers exercise prudent judgment, take a broad view, and apply common sense in their decisions.

EXAMPLE 26. FORMAL RESPONSIBILITIES OF A CRO WITH A STRENGTHENED ROLE

The problem that needed to be addressed:

Existing sound practice suggests that the CRO should have "sufficient seniority, voice, and independence from line business management to have a meaningful impact on decisions."³⁵ This has resulted in a marked strengthening of the role of the CRO and his/her direct reports, which has, in turn, been reflected in the CRO's key responsibilities.

How this firm went about addressing it:

- The bank's CRO is the head of the independent risk management function. The concentration and centralization of all risk functions allow for efficient group-wide risk control and capital management, which has reinforced the role of the CRO. This functional organization of risk responsibility, which is independent of the business segments within the bank, has improved risk management across risk types.
- The CRO is a Board member, which is the highest executive (management) decision-making level at the firm. The CRO reports directly to the Supervisory Board, including its risk committee.
- Several years ago, the firm implemented a risk governance model based on committees to discuss and take decisions on the firm's material risks. In recent years, these committees have evolved into the sole venue to seek approval to take on risk. The group risk committees are empowered by the Board to take risk decisions, and all relevant business units are represented to ensure appropriate interaction with the risk function. The CRO as the chair drives the discussions and makes sure that decisions and their implementation are within the firm's risk management framework (i.e., the firm's risk culture and risk appetite). The evolution of this process had already started before 2007/2008, but has been considerably accelerated post crisis.
- Additionally, the risk function is represented on other committees in the bank that do have an impact on risk or risk management issues. The CRO has influence on bonuses as a member of the Compensation Committee and the risk function proposes "risk takers" within the deferred bonus system of the bank's compensation plan.
- Furthermore, recent modifications in the committees' structure have seen a more focused approach on specific topics, for example:
 - The Group Strategic Risk Committee was created in 2010 to concentrate on, for example, risk concentration, and has primary responsibility for

monitoring and management of risk on a portfolio level across all risk types. This committee reports to the Board and is chaired by the CRO, which ensures an efficient link between the different risk types and committees. Membership on this committee also includes the heads of all business lines.

- The formal creation of a Group Risk Management Committee which serves as a discussion and decision making panel across all risk departments with the CRO as chairman. This has further strengthened the role of the risk management function and the CRO by facilitating discussions and decision making across risk types and risk management departments.
- The CRO has a key role in setting risk appetite, along with the rest of the senior management and the Board. For example, as a member of the Board, the CRO discusses and approves all business and risk strategies, including quantitative limits at the bank level.
- The CRO plays a key role in the implementation of the firm's risk culture and has recently put several measures into place to encourage discussion within risk management. For example the CRO:
 - Outlines the vision, mission, and strategy for the risk function.
 - Holds (in)formal meetings with employees and managers of the risk function.
 - Organizes frequent visits to the local branches and subsidiaries to meet the risk managers.
 - Initiated and oversees the process of defining risk function values, which provides the basis for achieving a culture of risk awareness, conscientiousness, and learning.

Key Lessons:

- The firm has found that it was only really practical to have a primary and independent reporting line that ensures consistency and clarity in the decision-making process. The firm's risk governance rests upon a committee structure, which enhances communication, avoids isolated decisions, and allows all relevant and interested departments to be actively involved in the discussion and the decision-making process. This also was found to be the most effective form of interface with the business and senior management.
- It was found that the three lines of defense (business lines as first line of defense, the control functions including risk management, as second line of defense; and the internal and external audit functions as a third line) can be fully efficient only if the CRO has the necessary instruments or tools to communicate and support the risk management strategy. The CRO's

³⁵ CMBP report, 9.

independence and seat on the Board are two of these tools.

- There is still some way to go, and the current focus is for the CRO to:
 - Promote and encourage stronger cooperation between risk management and finance.
 - Provide further support for, and integration of, different risks.
 - Manage the new regulatory challenges.

EXAMPLE 27. CRO ROLE AND RESPONSIBILITIES

The problem that needed to be addressed:

- Strengthen the voice of risk and enable risk to challenge the business as an independent party.
- Provide expert risk/capital challenge and advice close to the decision-making bodies of the business.
- Keep close contact with the business to avoid "ivory tower" effects.

How this firm went about addressing it:

- The bank established independent CROs as members of the Executive and Management Committees. The principle is that independent CROs exist where capital is allocated by the Group Executive Committee and/or strategic decisions are taken, where material risks are managed or if there are specific legal or regulatory requirements.
- The role of the CRO is to ensure that the business operates within the risk and capital playing field as well as to help and enable the business to fully and effectively incorporate a risk and capital perspective in its decisions, and to effect cultural change.
- To fulfill this role, the CRO should be close to the business and involved in all the phases of the business management cycle:
 - Assist in determining the size of the playing field during the planning phase.
 - Provide advice and input (and calling time-out when proposed decisions go beyond the playing field) during the execution phase.
 - Monitor and provide oversight in parallel with the business.
- Moreover, the role of the CRO is strengthened by his presence in the business committees:
 - Membership on the Executive or Management Committees provides "consensual power" to the CRO. In practice, this "consensual power" is provided by empowering the Group CRO to call time-out on decisions outside the risk and capital playing field, triggering the need for the CEO to resolve issues or escalate them to the Audit, Risk, and Compliance Committee (Board level). The Group CRO can formally delegate calling time-out right to his local CROs. If a local CRO calls time-out, the local CEO has to resolve the issue or escalate one level up in the organization. Every time-out call by a local CRO is reported to the Group CRO.

- Membership of, or a standing invitation to attend, other high-level business committees, (e.g., Credit Acceptance Committee).
- The Group CRO plays an important role in several Group Committees, which include:
 - Membership of the Group Executive Committee and an internal reporting line to this committee.
 - Chairing the Group Risk Function Management Committee, which is mainly responsible for risk governance, and the Group Risk Committees, which is responsible for risk and capital monitoring by business activity.
 - A standing invitation to the Group Audit, Risk, and Compliance Committee and a separate reporting line to the chairman of the Audit, Risk, and Compliance Committee. The Group CRO has a formal quarterly dialogue with the Chair of the Audit, Risk and Compliance Committee and ad hoc dialogue, if required.
- Local CROs are appointed to bring risk management closer to the business. A dual reporting system exists for the local CRO, hierarchically reporting to the local CEO and functionally reporting to the Group CRO.
- Local CROs also play an important role in several local committees, they are:
 - Full members of the Management Committee in their area of responsibility (if there are risk committees at their management level, they chair them).
 - Members of the firm's Group Risk Function Management Committee (CROs of material business units only).
 - Report to the Local Audit, Risk and Compliance Committee, if one exists.
- Finding equilibrium between group interests and group legal requirements, and local interests and local legal requirements.

Key Lessons:

Implementation challenges:

- Clarifying the role of the CRO and implementing this role in the different risk decision-making processes, which required some change management effort.
- Finding the people with the right profile and mix of business/risk experience to fill the CRO role.
- Determining the training path for a new CRO.

Ongoing challenges:

- Keeping risk on the agenda of the business.
- Maintaining oversight of activities, both those on local level and those at the group level affecting the local level.

ANNEX II. PREVIOUS IIF RECOMMENDATIONS

REFERENCED IN SECTION 1. RISK CULTURE

IIF Recommendation (CMBP report)

Firms should implement controls to ensure that the governance structure that has been adopted is actually implemented in managing day-to-day business. The regular and predictable functioning of risk management and governance structures is a fundamental element of effective risk management.

IIF Recommendations (SCI report)

Risk culture can be defined as the norms and traditions of behavior of individuals and of groups within an organization that determine the way in which they identify, understand, discuss, and act on the risks the organization confronts and the risks it takes.

Management should take an active interest in the quality of the firm's risk culture. Risk culture should be actively tested and objectively challenged in a spirit of fostering greater resilience and encouraging continuous improvement, reflecting the strategic aims of the organization.

Firms should ensure that relevant personnel have their formal responsibilities for risk clearly elaborated in their job descriptions and are evaluated for their fulfillment of these responsibilities as part of firms' periodic performance review.

Any material merger or acquisition should be the occasion of a serious analysis of the risk culture in the new organization; the opportunity to take action to correct problems and foster a positive risk culture should not be overlooked.

Firms should move to adapt risk-alignment concepts such as deferrals and claw backs to their own business models in light of prevailing regulatory and market environment.

REFERENCED IN SECTION 2. RISK APPETITE

IIF Recommendations (CMBP report)

When defining its risk appetite, the firm should be able to demonstrate consideration of all relevant risks, including non-contractual, contingent, and off-balance-sheet risks; reputational risks; counterparty risks; and other risks arising from the firm's relationship to off-balance sheet vehicles (see conduits and liquidity section).

IIF Recommendations (SCI report)

The finance and treasury functions should operate in a coordinated and cohesive manner with the risk management function to ensure important checks and balances.

The firm's risk appetite should be connected to its overall business strategy (including assessment of business opportunities), liquidity and funding plan, and capital plan. It should dynamically consider the firm's current capital position, earnings plan, liquidity risks, and ability to handle the range of results that may occur in an uncertain economic environment. It is fundamental, therefore, that the risk appetite be grounded in the firm's financials and liquidity profile. The appropriateness of the risk appetite should be monitored and evaluated by the firm on an ongoing basis.

Firms should involve the risk management function from the beginning of the business planning process to test how growth or revenue targets fit with the firm's risk appetite and to assess potential downsides. There should be clear communication throughout the firm of the firm's risk appetite and risk position.

Risk appetite should be the basis on which risk limits are established. Limits need to cascade down from the firm-wide level to business lines and divisions, to regions, and to trading desks. Risk-appetite usage should be measured on a global, consolidated basis and constantly monitored against the limits.

A firm's risk appetite will contain both qualitative and quantitative elements. Its quantitative elements should be precisely identified, including methodologies, assumptions, and other critically important information required to understand risk appetite. Clearly defined qualitative

elements should help the Board and senior management assess the firm's current risk level relative to risk appetite as adopted. Further, by expressing various elements of the risk appetite quantitatively, the Board can assess whether the firm has performed in line with its stated risk appetite.

The Board should review and periodically affirm, based on updates to risk metrics and similar guidance and information, the firm's risk appetite as proposed by senior management at least once a year. In so doing, the Board should assure itself that management has comprehensively considered the firm's risks and has applied appropriate processes and resources to manage those risks.

IIF Recommendations (Risk Appetite report)

- A strong risk culture³⁶ is a prerequisite to eventually putting in place an effective Risk Appetite Framework (RAF), and is also itself reinforced by the introduction of such a framework. Firms with demonstrably robust risk cultures that support "tone from the top" are best equipped to build engagement and put in place effective structures. One important implication of this is that an RAF should not be seen as a discrete set of mechanisms or processes, but rather as something inextricably linked to a wider set of issues that govern a firm's risk culture.
- It is essential that the determination of risk appetite is inextricably linked to strategy development and business plans, otherwise the two will rapidly come into conflict, creating significant tensions, and the conduct of business activities may lead to risk outcomes that, in aggregate, are outside acceptable boundaries. It is important to note that our study has shown that leading banks have made this linkage in an effective way. Formal involvement of the risk management function in the strategy and business planning processes has resulted in great benefits, which are evident in some of the case studies supplied.
- RAFs call for the use of extensive judgment on the part of Boards and management, in terms of where to begin, where to focus, and how to engage business leaders. Diverse risk cultures and business models, as well as differing degrees of complexity, mean that this is definitely an area in which one size does not fit all. While some convergence of practices can be expected to emerge over time, diversity of approaches among firms with different business models and risk profiles is inevitable, legitimate, and desirable.
- A risk appetite framework provides a context for such

traditional risk management tools as risk policies, limits, and management information based on clear risk metrics. An RAF should never aim to supplant these but can provide the framework within which conventional controls operate and can promote a better understanding and acceptance of their rationale and importance.

- Developing a risk appetite framework requires significant time and intellectual resources. The firms that have made the most progress report a substantial element of "learning by doing" in an iterative manner over time, and that ongoing dialogue and communication at all levels of the firm have been crucial in this process. Risk appetite cannot be implemented through top-down decrees, but instead needs to be embraced and understood throughout a firm. Business leaders need to be given time to define and embed the concepts of risk appetite into their decision-making processes, and this engagement takes time to evolve and mature. For this reason, the creation and evolution of a strong risk appetite framework is a multiyear journey—results do not appear instantly.
- An important implication of the above is that, in assessing firms' commitment to, and progress in, the implementation of a risk appetite framework, it is not possible to look at a simple and uniform set of indicators. Supervisors and internal stakeholders are encouraged to take a broad and multidimensional view in making assessments in this area.
- Clarity regarding the ownership of risk is essential. To ensure the broad congruence of business and risk decisions and the overall, enterprise-wide risk appetite, business heads should have visible ownership of risk in their areas and incorporate risk explicitly in their business planning. In fact, responsibility for the articulation and management of risk appetite within the businesses needs to reside firmly and clearly with business unit leaders—not with their embedded risk management staff—along with the ownership of the actual risks in the businesses. The risk management function should own the overall RAF, serve in an advisory capacity, and lead the interface with the Board on risk appetite.
- Communication is a key enabler, both in the development of an effective RAF and in its effective operation. Regular dialogue about risk appetite and evolving risk profiles needs to occur among the Board, senior management, the risk management function, and the businesses. This dialogue needs to encompass the development and evolution of the framework itself as well as the risks that are being taken throughout the businesses and the extent to which these (individually and collectively) conform to the overall risk appetite.

³⁶ The strong link between risk culture and the risk appetite framework also was highlighted in the December 2009 IIF report, *Reform in the Financial Services Industry: Strengthening Practices for a More Stable System*, in which the following generic definition was provided: "Risk culture can be defined as the norms and traditions of behavior of individuals and of groups within an organization that determine the way in which they identify, understand, discuss, and act on the risks the organization confronts and the risks it takes."

There is also significant value to be gained from communicating risk principles to broad employee audiences. The promulgation of agreed-upon key risk appetite themes needs to come from the top, and professionals within the risk management function can also act on opportunities to illustrate risk principles and explain and motivate the boundaries of risk appetite in day-to-day interactions with front-line staff.

- Firms that report the most progress in risk appetite practices benefit from strong collaboration among their risk management, finance, and strategy functions. Such collaboration is fundamentally required during the development of statements of risk appetite and the design of a risk appetite framework, but it is equally important in the day-to-day operation of an RAF. While the Board has final responsibility for risk matters, this is emphatically not about the Board making decisions about risk in isolation that are then handed down as instructions to the businesses. Rather, it is about developing an iterative and collaborative process for creating a framework and shared understanding about the boundaries of acceptable risk—both individually and in aggregate—that forms the basis of continuous dialogue and decision-making about preferred risk/return tradeoffs at all levels in a firm.
- Stress and scenario testing are important components of a risk appetite framework. Specifically, consciously constraining aggregate risks in advance in such a way as to ensure a firm's survival under severe macroeconomic, market and liquidity stress scenarios is at the heart of setting risk appetite appropriately. The choice of stress scenarios needs to balance the need to focus attention on severe outcomes while not placing impossible requirements on the businesses. This is a very important element of management and Board judgment, along with assessing the results of the stress tests and deciding on business and strategic adjustments that may be necessary to ensure that plausible losses under severe scenarios would be held to acceptable levels within the risk appetite framework. The individual stress and scenario testing capabilities of firms vary widely today, and our work has shown that firms are currently taking diverse approaches to using these tools for determining risk appetite. Specifically, some firms are using extensive stress and scenario testing in a very fundamental way in the determination of their risk appetite, whereas others are using these tests only to "sense-check" their overall risk appetite, or (in some cases) not at all. Consequently, this is a challenging area in which industry practices are still evolving and further guidance is needed, but there is agreement that stress testing results need to be incorporated into the determination of aggregate risk appetite in a very fundamental way.
- Board directors should set the framework for risk appetite and put into place mechanisms to ensure that decision-making will be consistently and transparently guided by it. But this is only the beginning of the process. Effective RAFs involve a highly iterative approach, with ongoing discussions of risk involving senior management and the businesses, and must be rooted in a strong risk culture. Engagement and challenge by the Board are key to achieving the right balance between rigidity and flexibility in the risk appetite framework; this is necessary if the framework is to be both workable and a meaningful source of discipline.
- Senior management should provide visible support and own the development of the RAF. Behaviors need to be continually and transparently consistent with the risk appetite principles that have been enunciated at the top. Business leaders need to articulate risk appetite in ways that are both tailored to their business strategies and operations and consistent with the enterprise-wide RAF, and they need to establish appropriate controls and reporting to manage risk.
- The risk management function needs to be actively involved at all levels of the development of the RAF and its operation. In its advisory capacity, this function adds value by being a catalyst for effective conversations with business leaders about risk and reward. It also is critical that risk management also develop supporting risk frameworks, policies, and reporting capabilities that enable business leaders to own and enhance their RAFs.
- Supervisors are encouraged to take a broad perspective when forming views regarding firms' commitment to, and progress in, the implementation of RAFs. The process is complex and time consuming, and it touches fundamentally on culture and behaviors in organizations. Assessments of commitment and success need to reflect this complexity. Successful outcomes are not reflected in the creation of ever more granular limit structures, and no single set of indicators or checklists can capture individual firms' progress in this area.

REFERENCED IN SECTION 3. ROLE OF THE BOARD AND BOARD RISK COMMITTEES

IIF Recommendation (CMBP report)

Boards have an essential oversight role in risk management. In attending to this duty, each Board should:

- Include members who have an adequate understanding of risk management. Each Board should be given the means to understand the risk profile of the firm and the firm's performance against it;
- Consider, depending on the characteristics of the firm, whether there should be separate audit and risk committees and whether at least some members of the risk committee (or equivalent) should be individuals with technical financial sophistication in risk disciplines;
- Set basic goals for the firm's risk appetite and strategy, such as ratings or earnings-volatility targets, with senior management and as guideposts for senior management in implementing risk management policies throughout the firm; and
- Review with senior management how the firm's strategy is evolving over time and when and to what extent the firm is deviating from that strategy (e.g., when a strategy resulted in heavy dependence on conduits or on structured products).

Firms should establish clear policies so that control and audit functions are independent of organizations whose activities they review. Their responsibility is to provide assurance that line businesses and the risk management organization are complying with internal and regulatory policies, controls, and procedures concerning risk management.

Firms should develop internal management procedures that make stress testing part of the management culture, so that its results have a meaningful impact on management decisions. Such procedures should discourage mechanistic approaches and promote a dialogue among the business, senior management, and risk function as to the types of stress tests to be performed, the scenarios most relevant, and the impact assessment of such tests (including the consideration of stress-testing results at the moment of determining the risk appetite of the firm).

Stress testing should play an integral role in assessing the firm's risk profile in relation to its risk appetite and be done across all business activities, risk types, and exposures.

Firms should reinforce procedures promoting active discussion between senior management and risk management as to the tests to be performed, the scenarios to be tested, and their implications for the firm. Strong feedback loops are essential in any robust stress-testing methodology. Equally important, methodologies should

take into account the relationships between stresses and valuation effects.

REFERENCED IN SECTION 4. ROLE OF THE CRO

IIF Recommendations (CMBP report)

Risk management should be a priority for the whole firm and not be focused only on particular business areas or made a purely quantitative oversight process or an audit/control function. Mutually reinforcing roles within each organization are essential to creating a strong, pervasive risk culture.

Risk management should be a key responsibility of the entire business-line management, not just of those businesses that invest the capital of the firm on a proprietary basis.

All employees in each organization should have a clear understanding of their responsibilities in regard to the management of risks assumed by the firm and should be held accountable for their performance with respect to these responsibilities.

Firms should define the role of the CRO in such a way that, without compromising his or her independence, he or she is in frequent interaction with the business lines so that the CRO and all risk managers have sufficient access to business information.

Firms should establish clear policies that define risk management as the responsibility of each institution's senior management, in particular the CEO, subject to the oversight of the Board. Senior management should be involved in the risk-control process, and both the Board and senior management should regard risk management and control as essential aspects of the business.

The CRO should have a sufficient degree of autonomy, be independent of line business management, and have sufficient seniority and internal voice in the firm to have a meaningful impact on decisions.

CROs should have a mandate to bring to the attention of both line and senior management or the Board, as appropriate, any situation that is of concern from a risk management perspective or that could materially violate any risk-appetite guidelines.

The CRO should report to senior management and, as appropriate, to the Board or its risk committee, on material concentrations as they develop, discuss material market imbalances, and assess their potential impact on the firm's risk appetite and strategy. The CRO should ensure a thoughtful, integrated view of the overall risks faced by the firm (including related off-balance-sheet vehicles).

At a more technical level, the risk management function

should oversee internal risk-rating systems, segmentation systems, and models, and to ensure that they are adequately controlled and validated. Assumptions behind models, grading systems, and other components of quantification should be recognized, and appropriate updates should be made when assumptions no longer hold.

The CRO and risk management function should be a key part of analyzing the development and introduction of new products, including the extension of products into new markets. New products with risk exposure, including those for which the bank accepts contingent liquidity or credit exposure, should be explicitly approved by the risk organization.

While firms retain freedom to determine their internal structures, firms should strongly consider having the CRO report directly to the CEO and assign the CRO a seat on the management committee. The CRO should be engaged directly on a regular basis with the risk committee of the Board. Regular reporting to the full Board to review risk issues and exposures is generally advisable, as well as more frequently to the risk committee.

Firms should consider assigning the following key responsibilities to the CRO:

- Guiding senior management in their risk management responsibilities;
 - Bringing a particularly risk-focused viewpoint to strategic planning and other activities of senior management;
 - Overseeing the risk management organization;
 - Assessing and communicating the institution's current risk level and outlook;
 - Strengthening systems, policies, processes, and measurement tools as needed to provide robust underpinnings for risk management;
 - Ensuring that the firm's risk levels and business processes are consistent with the firm's risk appetite, internal risk policies, and regulatory requirements for risk management; and
- Identifying developing risks, concentrations, and other situations that need to be studied through stress testing or other techniques.

Each firm should assign to the senior management-level the responsibility for risk management across the entire organization. In most cases, this would be to the CRO, although institutions may structure themselves differently to accomplish the same end.

IIF BOARD OF DIRECTORS

Vice Chairman
Roberto Setubal * +
President & CEO
Itaú Unibanco Banco S/A and
Vice Chairman of the Board
Itaú Unibanco Holding S/A

Chairman
Douglas Flint *
Group Chairman
HSBC Holdings plc

Vice Chairman
Walter Kielholz *
Chairman of the Board of Directors
Swiss Re Ltd.

Vice Chairman
Richard Waugh *
President and
Chief Executive Officer
Scotiabank

Vice Chairman and Treasurer
Marcus Wallenberg *
Chairman of the Board
SEB

Hassan El Sayed Abdalla +
Vice Chairman and Managing Director
Arab African International Bank

Federico Ghizzoni
Chief Executive Officer
UniCredit Group

Walter Bayly +
Chief Executive Officer
Banco de Crédito del Perú

Francisco González *
Chairman and CEO
BBVA

Martin Blessing
Chairman of the Board of Managing
Directors
Commerzbank AG

James Gorman
Chairman and CEO
Morgan Stanley

Gary Cohn
President and COO
The Goldman Sachs Group, Inc.

Piyush Gupta +
Chief Executive Officer and Director
DBS Group Holdings & DBS Bank Ltd

Ibrahim Dabdoub *+
Group Chief Executive Officer
National Bank of Kuwait

Gerald Hassell
Chairman and CEO
BNY Mellon

Charles Dallara (ex officio) *
Managing Director
Institute of International Finance

Jan Hommen
Chairman of the Executive Board
ING Group

Yoon-dae Euh
Chairman and CEO
KB Financial Group

Anshu Jain
Co-Chairman of the Management Board
and the Group Executive Committee
Deutsche Bank AG

* ANC Member + EMAC Member

Jiang Jianqing

Chairman of the Board & President
Industrial and Commercial Bank of China

Chanda Kochhar +

Managing Director and CEO
ICICI Bank Ltd.

Nobuo Kuroyanagi *

Senior Advisor
The Bank of Tokyo-Mitsubishi UFJ, Ltd.

Jacko Maree +

Group Chief Executive
Standard Bank Group Ltd

Masayuki Oku

Chairman of the Board
Sumitomo Mitsui Financial Group

Frédéric Oudéa

Chairman and CEO
Société Générale

Vikram Pandit *

Chief Executive Officer
Citigroup Inc.

Baudouin Prot *

Chairman of the Board
BNP Paribas

Urs Rohner

Chairman of the Board of Directors
Credit Suisse AG

Suzan Sabanci Dincer +

Chairman and Executive Board Member
Akbank T.A.S.

Peter Sands *

Group Chief Executive
Standard Chartered PLC

Yasuhiro Sato

Group CEO & Chairman of the Board
Mizuho Financial Group

Martin Senn

Group Chief Executive Officer
Zurich Insurance Group

Michael Smith

Chief Executive Officer
Australia and New Zealand Banking Group Ltd

James (Jes) Staley

Chairman
Corporate & Investment Bank
J.P. Morgan Chase & Co.

Andreas Treichl

Chairman of the Management Board
and Chief Executive
Erste Group Bank AG

Axel Weber

Chairman
UBS AG

Peter Wallison, Board Secretary

Arthur F. Burns Fellow
in Financial Policy Studies
American Enterprise Institute

IIF COMMITTEE ON GOVERNANCE AND INDUSTRY PRACTICES

Chairman

Mr. Richard Waugh

President and Chief Executive Officer
Scotiabank

Mr. Kevin Garvey

Head of Group Credit Review & Reporting
AIB Group

Mr. Edward Murray

Partner
Allen & Overy LLP

Mr. Nigel Williams

Chief Risk Officer
ANZ Banking Limited

Mr. Roberto Sobral Hollander

Department Director, Risk Department
Banco Bradesco S.A.

Mr. Alex Wolff

Head of Risk Strategy
Bank of Ireland

Mr. Antonio Rios Zamarro

Head of Global Risk Management
Bankia

Mr. Desmond McNamara

Managing Director Capital & Analytics, Group Risk
Barclays PLC

Mrs. Mayte Ledo Turiel

Head of Financial Trends and Relations with Regulators
and Supervisors, Finance Department
BBVA

Mr. Christian Lajoie

Head of Group Prudential Affairs
BNP Paribas

Mr. Brian Rogan

Vice Chairman and Chief Risk Officer
BNY Mellon

Mr. James Garnett

Head of Risk Architecture
Citi

Mr. Andrew Jennings

Managing Director, Basel II Regulatory Liaison,
Risk Architecture
Citi

Mr. Edward Greene

Partner
Cleary Gottlieb Steen & Hamilton LLP

Mr. Christian Wältermann

Group Market Risk Management; Head of Market Risk
Operations
Commerzbank AG

Mr. Andreas Blatt

Managing Director, Head Chief Risk Officer (CRO) IT
Credit Suisse

Mr. Roland Schmid

Managing Director, Chief Risk Office
Credit Suisse

Mr. Tonny Andersen

Member of the Executive Board
Danske Bank A/S

Mr. A. Scott Baret

Partner
Deloitte

Mr. Andrew Procter

Global Head of Government & Regulatory Affairs,
Government & Regulatory Affairs
Deutsche Bank AG

Mr. Bjørn Erik Næss

Group Executive Vice President/Chief Financial Officer,
Group Finance and Risk Management
DNB

Dr. Florian Strassberger

Global Head, Financial Institutions
DZ Bank

Ms. Patricia Jackson

Partner, FS Risk
Ernst & Young

Ms. JB King

Director
Ernst & Young

Mr. Robin Vince

Head of Operations
Goldman Sachs & Co.

Ms. Bárbara Frohn Verheij

Managing Director, Advisor to the CEO, Risk Division/
Public Policy
Grupo Santander

Mr. Saleem Sheikh

Chief Risk Officer/General Manager, Risk Management
Gulf Bank Ksc

Mr. Rakesh Jha

Deputy CFO
ICICI Bank

Mr. Jan van de Wint

Head of CCRM/Credit Capitals & Retail Risk
Management, Corporate Credit Risk Management
ING

Mr. Henk Huisman

Deputy Director
Public and Government Affairs
ING Group

Mr. Mauro Maccarinelli

Head of Market Risk Management, Risk Management
Department
Intesa Sanpaolo S.p.A

Mr. Robert Stribling

Director - Group Market & Risk Control
Itau Unibanco S/A

Mr. Adam Gilbert

Managing Director, Head of Regulatory Policy
JPMorgan Chase

Dr. Bart Delmartino

Risk Advisor, Group Value Risk & Capital Management
KBC

Dr. Mark Lawrence

Managing Director
Mark Lawrence Group

Mr. Philipp Härle

Director
McKinsey & Company

Ms. Monika Mars

Expert Associate Principal
McKinsey & Company

Mr. Fernando Figueredo Márquez

Global Chief Risk Officer, Global Risk Management
Mercantil Servicios Financieros

Mr. Toshinao Endou

Manager, Office of Basel III & International Regulation,
Corporate Planning Division
Mitsubishi UFJ Financial Group, Inc

Mr. Morio Iwata

Senior Manager, Corporate Planning Division
Mitsubishi UFJ Financial Group, Inc.

Mr. Kenji Fujii

Executive Officer, Head of Global Risk Management
Mizuho Securities Co., Ltd.

Mr. Naoaki Chisaka

Senior Vice President, Group Planning Division
Mizuho Financial Group, Inc.

Ms. Jane Carlin

Managing Director
Morgan Stanley

Mr. Parkson Cheong

Group Chief Risk Officer, Group Risk Management
National Bank of Kuwait S.A.K.

Mr. Scott McDonald

Managing Partner, Financial Services
Oliver Wyman

Mr. Phil Rivett

Partner
PricewaterhouseCoopers LLP

Mr. Morten Friis

Chief Risk Officer
Royal Bank of Canada

Mr. Kevin Nye

Senior Vice President, Enterprise Risk, Group Risk Management
Royal Bank of Canada

Mr. Nathan Bostock

Head of Restructuring and Risk
Royal Bank of Scotland

Mr. Steven Oon

Head of Firm Wide Risk Management
Royal Bank of Scotland

Mr. Robert Pitfield

Group Head, Chief Risk Officer, Global Risk Management
Scotiabank

Mr. Pierre Mina

Head of Group Regulation Coordination, DGLE/CRG
Société Générale

Mr. Clifford Griep

Executive Managing Director, Risk & Policy Officer, Ratings Risk Management
Standard & Poor's

Mr. Paul Smith

Group Head Governance and Assurance
Standard Bank of South Africa

Mr. Robert Scanlon

Group Chief Credit Officer, Group Chief Credit
Standard Chartered Bank

Mr. Nobuaki Kurumatani

Managing Director
Sumitomo Mitsui Banking Corporation

Mr. Clayton Herbert

Group Chief Risk Officer
Suncorp Group

Mr. Philippe Brahin

Head of Governmental Affairs, Regulatory Affairs
Swiss Re Ltd.

Ms. Ozlem Oner Ernart

Manager, Risk Management – Credit & Subsidiaries Risk
T.Garanti Bankasi

Mr. Takashi Oyama

Counsellor on Global Strategy to President and the Board of Directors
The Norinchukin Bank

Mr. Richard Metcalf

Group Managing Director and Group Risk Chief Operating Officer
UBS AG

Mr. Fabio Arnaboldi

Head of Group Risks Control, Group Risk Management
UniCredit SpA

Mr. Dominic O'Hagan

Executive Vice President & Chief Credit Officer, International Group
Wells Fargo & Company

Mr. Axel Lehmann

Group Chief Risk Officer, Regional Chairman Europe & Member of Group Executive Committee
Zurich Insurance Group

IIF RISK GOVERNANCE TASK FORCE

Chairman

Mr. Jacobus (Koons) Timmermans

Vice-Chairman
ING Bank

Mr. Jan Lubbe
Chief Risk Officer
Absa Group Limited

Mr. Thomas Wilson
Chief Risk Officer, Group Risk
Allianz SE

Mr. Jean-Christophe Menioux
Chief Risk Officer, Group Risk Management
AXA Group

Ms. Janelle Thibau
International Government Relations, Public Policy
Bank of America

Ms. Joan Mohammed
SVP, Central Risk Group
Bank of Montreal

Mr. Domingo Armengol Calvo
Corporate Secretary
BBVA

Mr. Christian Lajoie
Head of Group Prudential Affairs
BNP Paribas

Mrs. Mayalie Bonnin-Trentesaux
Director, Risk Management
Commerzbank

Mr. Christian Wältermann
Group Market Risk Management; Head of Market Risk
Operations
Commerzbank AG

Mr. Edwin Tan
Senior Vice President
DBS Bank Ltd

Mr. Henry Ristuccia
Partner
Deloitte

Mr. A. Scott Baret
Partner
Deloitte

Mr. Eddie Barrett
Director
Deloitte

Mr. Jay Mao
Director
Enterprise Risk Services
Deloitte

Mr. Stuart Lewis
Chief Risk Officer
Deutsche Bank

Ms. Shawn Gamble
Managing Director, Head of ICAAP / Risk Culture,
Enterprise Risk Management
Deutsche Bank AG, Filiale London

Ms. Patricia Jackson
Partner, FS Risk
Ernst & Young

Mr. Martin Rohmann
Head of Group Risk Management, Group Strategic Risk
Management
Erste Group Bank AG

Mr. Jaco Grobler
Chief Risk Officer, Enterprise Risk Management
FirstRand Bank

Ms. Bárbara Frohn Verheij

Managing Director, Advisor to the CEO, Risk Division/
Public Policy
Grupo Santander

Mr. John Woodhams

Group Head of Pension and Regulatory Risk, Group Risk
HSBC Holdings plc

Mr. Henk Huisman

Deputy Director, Public and Government Affairs
ING Group

Dr. Sérgio Werlang

Executive Vice President, Risk and Financial Control
Itaú Unibanco S/A

Mr. Robert Stribling

Director – Group Market Risk & Liquidity Control
Itaú Unibanco S/A

Mrs. Robin Doyle

Sr. Vice President, LOB CFO
J.P. Morgan Chase & Co.

Mr. Adam Gilbert

Managing Director, Head of Regulatory Policy
JPMorgan Chase

Ms. Lidia Luba

Group Senior General Manager of Value & Risk
Management
KBC

Dr. Mark Lawrence

Managing Director
Mark Lawrence Group

Ms. Cindy Levy

Director
McKinsey & Company

Ms. Monika Mars

Expert Associate Principal
McKinsey & Company

Mr. Fernando Figueredo Márquez

Global Chief Risk Officer, Global Risk Management
Mercantil Servicios Financieros

Mr. Stanley Talbi

Executive Vice President & CRO, Financial & Risk
Management
MetLife

Mr. Shiro Katsufuji

Chief Manager, Corporate Risk Management Division
Mitsubishi UFJ Financial Group, Inc.

Mr. Kenji Fujii

Executive Officer, Head of Global Risk Management
Mizuho Securities Co., Ltd.

Mr. Naoaki Chisaka

Senior Vice President, Group Planning Division
Mizuho Financial Group, Inc.

Mr. Kouhei Kuroda

Deputy General Manager, Risk Management
Mizuho Financial Group, Inc.

Mr. Lionel Burger

Enterprise Risk manager
Nedbank

Mr. George Stylianides

Partner, Consulting, Financial Services Risk Leader for
Europe, Middle East, Africa and India (EMEA)
PricewaterhouseCoopers LLP

Mr. Kevin Nye

Senior Vice President, Enterprise Risk, Group Risk
Management
Royal Bank of Canada

Mr. Robert Pitfield

Group Head, Chief Risk Officer, Global Risk
Management
Scotiabank

Mr. Paul Hartwell

Group Chief Risk Officer, Risk
Standard Bank

Mr. Robert Scanlon

Group Chief Credit Officer, Group Chief Credit
Standard Chartered Bank

Mr. Yoshiyuki Ohmi

Chief Risk Officer & General Manager, Risk Management
Department
Sumitomo Mitsui Banking Corporation Europe

Mr. Toshio Mano

Deputy General Manager, Risk Management Department
Sumitomo Mitsui Banking Corporation Europe

Ms. Patricia Brown
Joint General Manager
Sumitomo Mitsui Banking Corporation Europe

Mr. Clayton Herbert
Group Chief Risk Officer
Suncorp Group

Mr. Steve Snipes
Head Corporate Risks & Governance, Director
Swiss Re Ltd

Mr. Akihiko Kabe
Advisor for Risk Management of the Norinchukin Bank
The Norinchukin Bank

Mr. Richard Metcalf
Group Managing Director and Group Risk Chief
Operating Officer
UBS AG

Mr. Antonio Russo
Head of Credit Risk Policies, Group Risk Management
Unicredit

Mr. Fabio Arnaboldi
Head of Group Risks Control, Group Risk Management
UniCredit SpA

Ms. Subuola Abraham
Chief Compliance Officer
United Bank for Africa

Mr. Dean Saunders
Head of Risk Strategy and Governance, Group Risk
Westpac

Ms. Catherine Thrum
Senior Manager, Group Risk
Westpac

Mr. Axel Lehmann
Group Chief Risk Officer, Regional Chairman Europe &
Member of Group Executive Committee
Zurich Insurance Group

Dr. Carin Huber
Strategic Assistant to Group CRO, Group Risk
Management
Zurich Insurance Group



INSTITUTE OF INTERNATIONAL FINANCE

1333 H Street, NW, Suite 800 East
Washington DC 20005-4770

Tel: 202-857-3600 Fax: 202-775-1430

www.iif.com