Working slides

Society of Actuaries in Ireland

Overseeing Risk Management in a Financial Institution

Pat Ryan

25 September 2013

Foreword

There is more material in these slides than used in the presentation itself.

Extra content is included which provides some backup to the summary points given in the presentation

Introduction

I will cover three broad topics:

1. The regulatory background;

2. Lessons from financial failure – failings of Boards to ensure sound Risk and Compliance management; and

3. How Boards now need to oversee Risk, and interact with the function

1. Regulatory background

New regulatory landscape

- Increasing Central Bank focus on Governance, Risk Management and Compliance

- Increasing role of European Regulators, notably EIOPA and EBA

- Conduct of Business, regulatory and legal requirements intensifying

➢ **These, with supporting clarifications, are paramount in shaping the Board's perspective on Risk and Compliance oversight duties**

Role of Board

- Effective, prudent and ethical oversight;
- Setting the business strategy; and
- Ensuring that risk and compliance are properly managed

Central Bank Corporate Governance Code, November 2010

Role of the Board further specified

- Capital adequacy for the risks of the firm
- Robust and transparent organisational structure
- Remuneration framework in line with risk strategies
- Adequate and effective internal control framework

Central Bank Consultation Paper CP 69, August 2013

Central Bank's expectations of INEDs

- Competence, experience and skills to do the job
- Act and be seen to act independently
- Satisfy themselves that the strategy of the company is sound and the core business model is profitable and sustainable
- Insist risk/reward trade off clearly defined with clear risk appetite statement and risk limits, ongoing monitoring of risk, board level reporting of breaches
- Ensure there are clear processes, structures and controls in place to ensure effective governance – do not rely solely on management representation
- Champion adequate resourcing for and independence of the internal audit and risk management functions
- Hold management accountable for their actions and for ensuring implementation of the agreed strategy and risk framework

Central Bank of Ireland, November 2012

INED responsibility for Risk & Audit

Particular responsibility on INEDs in relation to risk management and audit

The non-executive directors and in particular independent non-executive directors shall play a leading role in the Board Risk Committee and the Board Audit Committee or where the functions are carried out at group level, they shall play a leading role in satisfying the board that the institution's audit and risk functions are adequately carried out.

Central Bank Corporate Governance Code, November 2010

Board skills and qualifications

- *The Chairman and the CEO are both required to have significant financial services expertise, qualifications and background.*

- *The INEDs must have a knowledge and understanding of the business, risks and material activities of the institution.*

- *The INEDs must comprise individuals with relevant skills, experience and knowledge to provide independent challenge*

- *The Board must have ...... a full understanding of the nature of the institution's business, activities and related risks.*

Central Bank Corporate Governance Code, November 2010

Board responsibilities for Risk Function

- *The Board Risk Committee shall oversee the risk management function.*

- *The Board Risk Committee shall ensure the development and on-going maintenance of an effective risk management system within the financial institution that is effective and proportionate.*

- *The board shall satisfy itself that all key Control Functions such as internal audit, compliance and risk management are independent of business units, and have adequate resources and authority to operate effectively.*

Central Bank Corporate Governance Code, November 2010

Three Lines Of Defence

The three lines of defence outlines the firm's internal risk management. Each line has specific responsibilities in respect of risk assessment, management, oversight, compliance and control

	1st Line (Risk Management)	2nd Line (Risk Control)	3rd Line (Risk Assurance)
Responsibilities	Identifying, assessing, managing and controlling the risks it takes or is exposed to while conducting its activities	Providing risk and compliance oversight to the business (but not for its management)	Providing independent assessment of risk and compliance management and internal control system
How does this apply for risk	Effective processes to identify, measure or assess, monitor, mitigate and report on risks	Develop and maintain systems and processes to identify, measure, manage, monitor and report on risks, and ensure prudent conduct of business and compliance with laws, regulations, supervisory requirements and internal policies and procedures.	Independent review of the activities of the first two lines of defence

2. Lessons from financial failure

How we got here

- There has been a huge and costly failure of Irish banking.
- Three large general insurance companies have failed since 1980, requiring vast financial support by way of levy on policyholders.
- Citizens, taxpayers and customers bear the cost of financial failure of banks and insurance companies - consequently, the community is entitled to take such actions as are needed to prevent such failures – this is the core reason for the special regulatory treatment of banks and insurance companies.
- The responsibilities for managing risk and compliance placed by the CB and by EIOPA and the EBA on boards of financial institutions reflect this reality, and are an intended barrier to future costly mistakes.

Inadequacy of skills at the top

*"In an important sense, the major responsibility lies with the **directors and senior managements of the banks** that got into trouble. They are the first line of defence to protect those who have entrusted them with their funds"*

Honohan Report

"Among Non-Executive Directors (NEDs), it appears that the banking knowledge and expertise necessary to assess the lending and funding risks inherent in bank business models was insufficient. They were therefore formally independent but, in practice, highly reliant on the knowledge, openness and ability of bank management"

"In general, while NEDs were successful and respected individuals from various parts of Irish business, not many of them were banking professionals or had comparative experience. Even though discussions on management proposals and reports were robust at times, actual rejections of business models, strategies and proposals were rare"

"The board members (of Anglo) were experienced and well regarded in their own fields of speciality. However, they were not expert in the field of banking"

Nyberg Report

Board inadequacies in Ireland

"This weakness in reporting processes was combined with a lack of sufficiently extensive banking experience and expertise at board level of the type which would have allowed the board to identify shortcomings in the information being provided"

"These issues were particularly problematic because most Anglo Board members did not appear to have sufficient experience or specialist knowledge to fully recognise the specific risks attaching to a fast-growing monoline bank"

"It is, nevertheless, incumbent on a board to have sufficient understanding and awareness of the risks associated with the business for which it has oversight responsibility on behalf of shareholders and others"

"The board must ensure that sufficient checks and balances are in place and operating effectively to assist the board to meet its responsibilities"

Nyberg Report

CONCLUSION. Complex financial firms need INEDs with a detailed understanding of the risks to which the firms are exposed, and with the background and knowledge to provide a robust challenge to management.

He felt that the role of Chairman of the Risk and Compliance Committee was too complicated for a generalist. It involved understanding complex and evolving international banking rules around the Basel Agreements. *Outgoing Chairman of Anglo Risk and Compliance Committee (June 2008), from Anglo Republic by Simon Carswell*.

Inadequacies in UK - HBOS

"The corporate governance of HBOS at Board level serves as a model for the future, but not in the way in which Lord Stevenson and other former Board members appear to see it. It represents a model of self-delusion, of the triumph of process over purpose"

"The strategy set by Board from the creation of the new Group sowed the seeds of its destruction"

UK Parliamentary Report

Weak Risk and Compliance - HBOS

"Sir James Crosby told us that his aim in creating the position of Group Risk Director was to enhance its profile and "enhance the position in the context of the Group". He nevertheless conceded that it was "unusual" that two successive holders of the new post had no specific experience in risk functions. Indeed, he conceded that it could be characterised as "bizarre".

"The weaknesses of group risk in HBOS were a matter of design, not accident. Responsibility for this lies with Sir James Crosby, who as Chief Executive until 2005 was responsible for that design, with Andy Hornby who failed to address the matter, and particularly with Lord Stevenson as Chairman throughout the period in question" "*

**successor CEO*

UK Parliamentary Report

Skills Inadequacies - HBOS

"There was insufficient banking expertise among HBOS's top management. In consequence, they were incapable of even understanding the risks that some elements of the business were running, let alone managing them"

"The non-executives on the Board lacked the experience or expertise to identify many of the core risks that the bank was running"

"Consumers and the wider economy, as well as shareholders and taxpayers, have paid a heavy price for the blunders of the HBOS Board"

UK Parliamentary Report

Barclays' Governance

"There was no clear home for Board oversight of operational risk, including the increasingly important category of conduct risk, although it came within the formal remit of the Board Risk Committee."

"Since compliance functions have significant controlling responsibilities as well as their advising responsibilities, maintaining their independence is particularly important to the effective execution of their mandate."

"We consider it important that Compliance is given sufficient authority within the organisation. Having the Group Head of Compliance on the ExCo helps this."

The Salz Review

Inadequacy of financial regulation

Observations on financial regulation set out in the three reports on the Irish banking failure include:

- *Nevertheless,……, the key protection in any national system against the emergence of a banking crisis should be the **central bank and regulatory function**. Honohan Report*
- *To be effective there would have had to be a **greater degree of intrusiveness and assertiveness** on the part of regulators in challenging the banks. Honohan Report*
- *The supervisory culture was insufficiently intrusive, and staff resources were seriously inadequate for the more hands-on approach that was needed. Regling-Watson Report*
- *Governance failures were not addressed sufficiently toughly. Regling-Watson Report*
- *Where risks, deficiencies or weaknesses were identified in processes and procedures, the Financial Regulator did not act forcefully to ensure that these issues were addressed. Nyberg Report*

The consistent theme of the three reports is that financial regulation is the last line of defence, and needs to be tough, intrusive and assertive.

This is now a new reality, with the Central Bank having significantly rewritten its rule-books and engaging to a much greater extent, and in a much more robust way, with regulated firms.

3. Board oversight and interaction

Board supports Risk by:

- Culture and Tone from the Top
- Clear and well articulated Risk Appetite
- Function’s direct line to the Board Risk Committee
- Function’s attendance at relevant Board Committee
- Active consideration of the Risk Agenda
- Ensuring function has independence and sufficient resources

Changing culture

- Tone from the Top
- Trust is a fundamental requirement
  - Customers and all other stakeholders
- Clearly articulated values
  - Supported at all levels
  - Lack of tolerance for breaches
- Linking risk and performance management

Risk appetite statement

- Earlier presentation today has been devoted to this subject
- However, its importance to the Board warrants reference here
  - Key mandate by the Board of business direction and boundaries
  - It merits considerable time being given to its formulation
  - Usually iterative process to get right
  - Use test is whether it sets the direction of business

Board expectation of CRO

- Independence of mind
- Sufficient stature and ability to partner with Senior Management
- Strategic and commercial awareness
- Forward focus
- Professionally qualified
- Supporting achievement of business objectives in a compliant way

Central Bank expectation of CRO

- Sufficient seniority and independence to challenge / influence
- Relevant expertise, qualifications and background
- Manage risk control function and monitor risk management framework
- Promote an appropriate risk culture
- Provide risk information to enable the Board understand overall risk profile
- Facilitate the setting of the risk appetite for the Board

Central Bank Consultation Paper CP 69, August 2013

Reinforced independence of CRO

- *"The CRO shall report to the board risk committee with direct access to Chairman of the board"*

Central Bank Consultation Paper CP 69, August 2013

- Primary accountability to Board is similar to corresponding FSA provision

- The FSA provides for a secondary executive reporting line:

  "FSA recognises that in addition to the CRO's primary accountability to the governing body, an executive reporting line will be necessary for operational purposes"

- EBA guidelines already require primary reporting line to the Board

Reporting line of the CRO

"The CRO shall report to the board risk committee with direct access to Chairman of the board"

Central Bank Consultation Paper CP 69, August 2013

- The Walker Review (November 2009), established "*in light of the experience of critical loss and failure throughout the banking system*", recommended that, "*in support of board-level risk governance*", banks and insurance companies should be required to have a CRO reporting to the Board Risk Committee.
- The FSA (now PRA) gave effect to that recommendation in May 2011, reflecting in its rule book "*the primacy of the CRO's accountability to the board*". The FSA also made provision for an "*executive reporting line for operational purposes, in addition to the Chief Risk Officer's primary accountability to the board*".
- In the case of banks, the EBA Guidelines on Internal Governance, which have had full regulatory effect since March 2012, require banks to have independent Control Functions, including a Risk Control function, a Compliance function and an Internal Audit function. The Guidelines state: *"In order for the control function to be regarded as independent , .. the head of the control function generally should report directly to the management body* **(i.e. the board)** *and any relevant committees and should regularly attend their meetings".* The proposed insertion in the Corporate Governance Code already applies to banks. Nonetheless, given the key role of the Corporate Governance Code, the inclusion of this requirement in it will enhance the status of the requirement.

Reporting line of the CRO

- It was arguably already implicit in the Code that the CRO's primary reporting responsibility was to the Board Risk Committee, particularly given that the Code requires that the Board Risk Committee shall oversee the risk management function. Nonetheless, making the requirement explicit in the Code will result in a more comprehensive and consistent structure in relation to oversight of the risk management function.
- On a related topic, it is also proposed to include in the Code a requirement that the Board Risk Committee be chaired by a non-executive director. The Central Bank states that this "*is supportive of the Board Risk Committee's role, inter-alia, in providing oversight of the risk management function*".
- Taken together, these two changes go a long way to ensuring that non-executive directors play a leading role in establishing that the risk function operates effectively and with independence.
- One of the key conclusions of the various reports and investigations on the financial crisis was that non-executive directors lacked the experience or expertise to identify the core risks being run, and thus could not provide effective challenge to, or oversight of, executive management. The Code now specifically requires that INEDs must have the experience or expertise necessary to identify core risks. The reporting line of the CRO to the Board Risk Committee will further support INEDs in providing risk oversight – the Walker Review recommended this structure "*in support of board-level risk governance*".

In summary, a good Risk function:

- Supports the Board
- Partners with Management while retaining independence
- Is robust in its challenge
- Is proactive identifier of potential risks
- Is well resourced with professionally qualified staff
- Produces high quality reports → Identifies key issues for Board

The alternative............?

Ghost of Christmas to come?