Chapter 3 The Governance of Risk Management

Version 1.0

Introduction

Corporate governance is defined as the method of managing and running companies. It describes the roles and responsibilities of a firm's shareholders, board of directors, and senior management.

This chapter describes how risk governance evolved from a vague principle into well-defined set of best practices driven by a series of high-profile corporate scandals such as Enron, WorldCom etc. These scandals let to regulatory reforms aimed at improving governance of public companies, increasing transparency and executive accountability, and improving financial controls and oversight.

Sarbanes-Oxley Act

In the US, regulatory reforms were enacted in the form of the 'Sarbanes-Oxley Act' (SOX). SOX was implemented in 2003 and it created stricter legal requirements for boards, senior management, as well as external and internal auditors.

Some notable aspects of SOX are:

- Chief executive officers (CEOs) and chief financial officers (CFOs) must ensure that the financial reports filed with the SEC are accurate. They must personally verify and certify these reports.
- CEOs and CFOs must attest that disclosures provide an accurate picture of their company's financial conditions and operations.
- CEOs and CFOs are responsible for internal controls, including their design and management. They are also required to disclose any significant deficiencies in internal controls, as well as fraudulent activities to external and internal auditors.
- The effectiveness of a company's reporting procedures and controls must be evaluated on an annual basis.
- The names of individuals who serve on the board audit committee should be disclosed. These individuals should understand accounting principles, be able to comprehend financial statements, and have experience with internal audits.

Risk Management Failures During the 2007-2009 Financial Crisis

The 2007-2009 financial crisis was directly linked to several risk management failures. The crisis was triggered by a downturn in a previously 'hot' housing market. At the heart of the crisis were two key issues:

- Sub-prime mortgages: Lenders engaged in unsound business practices. They extended loans to unqualified individuals and encouraged homeowners to take on more debt than they could handle.

- Complex asset-backed securities: The sub-prime mortgages were securitized into complex asset-backed securities and sold in the mainstream credit market. The investment banks who originated and traded these securities as well as the rating agencies who assigned them credit ratings, failed to accurately assess their real risk and value.

Eventually, the subprime borrowers started defaulting and the associated mortgage-backed securities witnessed heavy losses. Several major investment banks that were holding these low-quality assets had to file for bankruptcy. This affected banking and economic activity all around the world. It became evident that a decline in underwriting standards, breakdown in oversight, and overuse of complex securitized products resulted in this crisis.

Key Post Crisis Corporate Governance Concerns of the Banking Industry

- Stakeholder priority: The focus of corporate governance in many industries is on maximizing shareholder benefit. However, in addition to shareholders, banks have several key stakeholders such as depositors, debtholders, and taxpayers. As compared to shareholders who may press for short-term results, these other stakeholders have a much stronger interest in minimizing the risk of bank failure. Risk management can be difficult due to these contradictory needs.
- Board composition: The crisis led to discussions on how bank boards can strike the right balance of independence, engagement, and financial industry expertise. An examination of failed banks revealed no apparent difference in outcome regardless of whether board members were insiders or outsiders.
- Board risk oversight: Following the crisis, it became clear that the board needs to be more proactive in risk management. This has resulted in a greater emphasis on educating boards about risk and ensuring that they maintain a direct link to the risk management infrastructure.
- Risk appetite: Banks should develop a formal, board-approved risk appetite that defines a firm's willingness to take risks. This can be used to set enterprise-wide risk limits.
- Compensation: Boards should exercise control over compensation schemes to prevent undesired risk-taking. For example, deferred bonus payments and clawback provisions can be implemented.

1. The Post Crisis Regulatory Response

The Basel Committee on Banking Supervision (BCBS) was formed to address the corporate governance concerns of the banking industry. It is an organization comprised of central banks and bank supervisors from 27 different countries. They created a set of standards which are presented below. These standards are not legally binding, but are incorporated voluntarily.

- Basel I: The Basel Accord (Basel I framework) was introduced in 1988 following the Latin American debt crisis. The prime focus was on managing credit risk. It introduced a risk-weighted approach to capital requirements and set the prescribed minimum capital at 8% of a firm's risk-weighted assets.
- Basel II: An enhanced version of the framework was launched in 2006 (Basel II). The Basel II framework incorporated both trading and lending activities in the calculation of risk. The 8% recommended minimum remained, but the risk-weighting methodology became more refined. Basel II also established standards for supervisory bank reviews and disclosure requirements in order to strengthen market discipline through transparency.
- Basel III: In response to the 2007-2009 financial crisis Basel III was introduced. This framework focuses on both firm specific risk and systemic risk. Systemic risk is defined as the risk of a major financial institution failing, resulting in the failure of the entire financial system.

Basel III

The Basel III framework limits a bank's Tier I capital to include common equity and retained earnings only. This raises the capital's quality. It also introduced two key ratios for short-term and long-term liquidity:

- Liquidity coverage ratio (LCR): Banks must hold enough highly liquid assets to fund 30 days' worth of cash needs.
- Net stable funding ratio (NSFR): Banks must have at least one year's worth of stable cash flow to fund required operations.

Finally, Basel III also designed a 'macroprudential overlay' with an objective to lessen systemic risk and procyclicality. This overlay consists of five elements:

1. A leverage ratio of 3%.
2. A countercyclical capital buffer.
3. Total loss-absorbing capital standards are applicable to all global systemically important banks.
4. To protect systemically important markets and infrastructures from counterparty risk, Basel III is pushing the market to move as many trades as possible through centralized clearing.
5. Systemic risk and tail events are being captured in risk modelling and stress testing.

Fundamental review of trading book (FRTB): In 2016, Basel III introduced FRTB to widen the framework for handling market risk. Specifically, disclosure requirements were strengthened to reflect a more thorough approach to describing and calculating risk, as well as to facilitate comparative risk analysis.

After the Crisis: Industry Restructuring and the Dodd-Frank Act

Until 1999, the Glass Stegall Act was in effect in the US, under which commercial banks and investment banks were separated by law. This was done with the objective of protecting depositors from trading volatility.

In 1999, the Graham-Leach-Bliley Act was launched which allowed bank holding companies to convert into financial services holding companies (FSHCs). This allowed commercial banking to be combined with investment banking, insurance and broker-dealer activities under one corporate umbrella.

The result of the removal of the Glass Stegall Act was that investment giants like Bear Stearns and Merrill Lynch were in such stress that they had to be merged with banking institutions and Lehman Brothers went bankrupt.

To address these issues and to improve consumer protection and systemic stability, the 'Dodd-Frank Act' was introduced in July 2010. The key elements of this act are presented below:

- Strengthening the Fed: The act gave the federal reserve oversight over all systemically important financial institutions (SIFIs). SIFIs are defined as bank holding firms with assets more than $50 billion.
- Ending too-big-to-fail: An orderly liquidation authority was created to put an end to 'too-big-to-fail" scenarios.
- Resolution plan: SIFIs are required to submit a 'living will' that outlines a corporate governance structure for resolution planning in times of distress.
- Derivatives markets: The act focused on making the derivatives market more transparent and reducing counterparty risk.
- The Volcker rule: This rule prohibited banks from engaging in proprietary trading and investing in hedge funds and private equity funds.
- Protecting consumers: A consumer financial protection bureau (CFPB) was created to regulate consumer financial services and products.
- Stress testing: The act introduced a completely new approach to scenario and stress testing. Some key points are listed below:
    - A top-down approach with a focus on macroeconomic factors and their impact on different types of risk.
    - A stress testing framework that is fully incorporated into a bank's business, capital, and liquidity planning processes.

- An approach that not only looks at each bank in isolation but also looks at the entire banking system collectively to see how a macroeconomic scenario will affect the system.
- Two stress testing exercises are conducted - the Dodd-Frank Act Stress Test (DFAST) for banks with assets greater than $10 billion, and the Comprehensive Capital Analysis and Review (CCAR) for banks with assets greater than $50 billion.

2. Infrastructure of Risk Governance

The Board and Corporate Governance

- Independent Board Members*:* BOD should comprise of a majority of independent members. The CEO and the chairperson of the board should be two different and independent people.
- Knowledgeable and experienced: All board members should possess basic knowledge of the firm's business and industry.
- Board should serve in the best interests of all stakeholders: The board should serve in the best interest of all stakeholders and not just the shareholders. This is not an easy task as stakeholder interests are not always the same.
- Manage Conflicts of interest well: Addressing conflict of interest between the management and shareholders is one of the core objectives of the board. This is referred to as agency risk which arises when the owners and operators of a business are different individuals.
- Board should be aware of any agency risks: Management may take on greater risks in order to maximize personal remuneration in the short term even if it hurts the firm in the long term.
- Responsible for designing management compensation plans: Management compensation plans should be well designed to keep executives from being tempted to prioritize short-term results over long-term goals.
- Board should also appoint a CRO: The CRO or Chief Risk Officer is the person who helps the board understand the firm's risk mapping and risk management process.

From Corporate Governance to Best-Practice Risk Management

Over the last two decades the objectives of corporate governance and risk management have converged. Risk governance involves setting up an organizational infrastructure to articulate formal procedures for defining, implementing and overseeing risk management.

The board of directors play a central role in the risk management process. The board must proactively participate in strategic planning and set up an appropriate risk appetite for the firm. This risk appetite should be clearly communicated throughout the firm.

The board should asses whether any major transaction undertaken by the firm is consistent with the authorized risk and associated business strategies.

The board must ensure that procedures for identifying, assessing, and managing various types of risk (business, operational, liquidity etc.) are in place. The board is ultimately responsible when risk policy is ignored or violated.

The board should take the decision of whether known risks should be retained, avoided, mitigated or transferred.

The board must evaluate the firm's compensation strategy. Executives should be compensated based on their risk-adjusted performance. Compensation incentives should not clash with shareholder interests.

The board should ensure that the information it receives about risk management implementation is accurate and reliable. It should gather information from a variety of sources, including the CEO, other senior executives, internal and external auditors.

The board should consist of a risk committee whose members have enough experience to analyze key risks properly. The board risk committee and audit committee should be two separate entities.

3. Risk Appetite Statement

An important component of corporate governance is publishing a risk appetite statement (RAS). RAS is defined as 'a written articulation of the aggregate level and types of risk that a firm will accept or avoid in order to achieve its business objectives'.

RAS includes both qualitative and quantitative statements. Its objectives should be clearly articulated. For example: Safeguarding our reputation and brand, Achieving/maintaining an AA rating etc.

4. Implementing Board-Level Risk Governance

The Board Audit Committee

The board audit committee oversees the firm's regulatory, legal, compliance, and risk management activities. It is accountable for the accuracy and completeness of a firm's financial and regulatory disclosures.

An audit provides the board with independent verification of whether the firm is doing what it claims to be doing.

Members of the audit committee must be knowledgeable, capable of making independent decisions, financially literate, and have the utmost integrity.

The Evolving Role of a Risk Advisory Director

Sometimes a company's board can include individuals who originate from other industries beyond the financial services sectors. In such cases, the board should appoint an independent risk advisory director who specializes in risk analysis and management. This person can advise the board on the best practices in corporate governance and risk

management. His primary responsibility is to improve the effectiveness of the risk and audit committees.

The Special Role of the Board Risk Management Committee

The risk management committee is responsible for setting the firm's risk appetite and independently monitoring the firm's risk management.

The committee maintains a direct contact with external and internal auditors which allows for better communication between the board and management.

The BOD typically delegates the responsibility for approving and reviewing risk levels to the risk management committee.

5. Risk Appetite and Business Strategy: The Role of Incentives

A firm's risk appetite should be defined to support the firm's business strategy and should be directly linked to the firm's strategic goals. However, the risk appetite should also reflect its tolerance to accept risk. For example, extending loans to subprime borrowers at high interest rates may be potentially profitable, but it may not fit the bank's risk tolerance limits.

Risk appetite is brought into operations through risk limits. The limits can be imposed at both the business-unit level and at the asset-class level. These limits can be monitored through stress testing or VaR. Some margin should be left so as to not trigger the limits on a daily basis.

Risk Supervision Hierarchy

The board is responsible for setting the enterprise level risk appetite through the risk committee. While the CRO (chief risk officer) is responsible for:

- Day-to day risk supervision and decisions
- Approving temporary breaches of limits imposed on the various business activities, provided these breaches remain within the overall enterprise-level board-approved limits.
- Acting as a liaison between the board and management.
- Reporting directly to the CEO, maintaining a seat on the board risk committee, and having a voice in approving new financial instruments and lines of business.
- Having a plan ready when risk limits are breached – for example, a CRO may order specific units to cut back or entirely close positions if there are concerns regarding exposures to market, credit, operational, or business risks.

6. Incentives and Risk-Taking

After the global financial crisis it became evident that executive compensation schemes at many financial institutions encouraged short-term risk taking, causing management to

sometimes entirely ignore long-term risks. Compensation schemes were structured like call options – they had unlimited upside but were capped on the downside.

Managerial Compensation Reforms

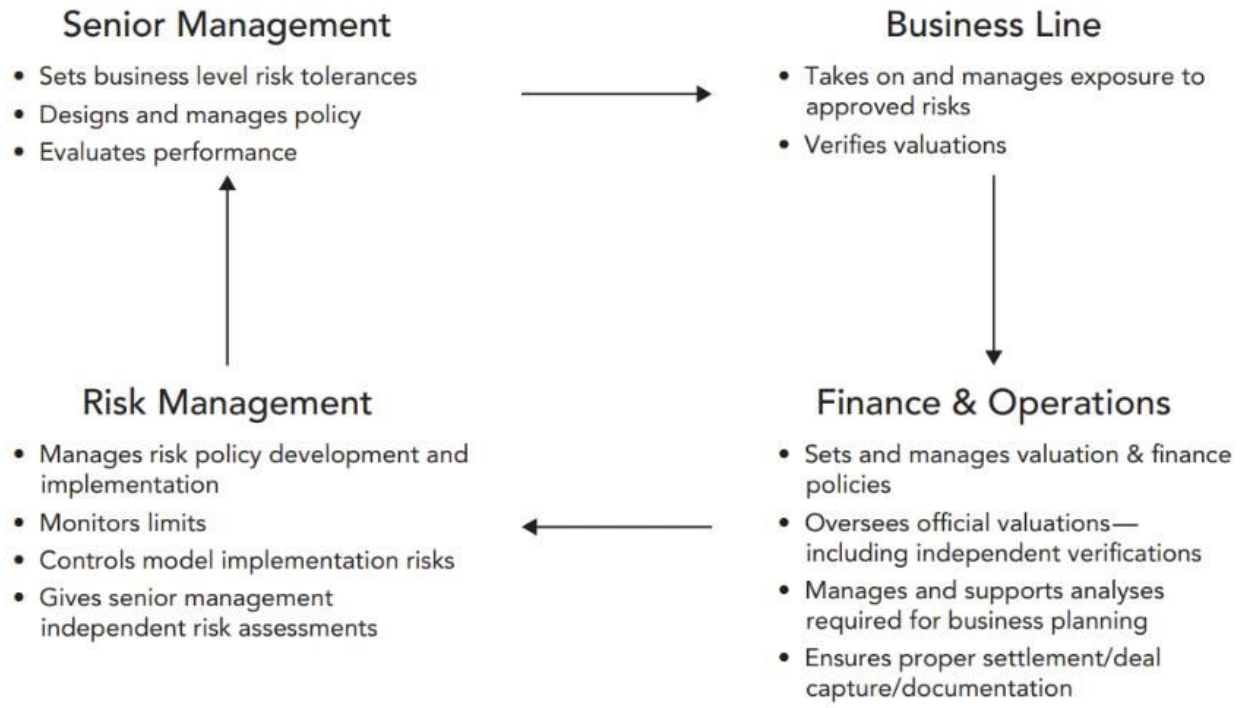
To address this issue, in September 2009, G-20 countries recommended the following managerial compensation reforms:

- Eliminating multi-annual guaranteed bonuses.
- Incorporating downside exposure by deferral of certain compensation, adoption of share-based remuneration, clawback provisions. These structures incentivize long-term value creation.
- Limiting the amount of variable compensation granted – for example, bonus caps equal to 100% of an executive's salary, or if approved by 2/3rd shareholders a bonus equal to 200% of base salary.
- Improving the disclosure requirements to make compensation packages more transparent.
- Affirming the independence of the compensation committee

Share-based compensation align the interest of executives and shareholders. While this structure is better than call options, in some situations this can still encourage risk-taking because shareholder gains are infinite, while their losses are limited to their investment. To prevent this, some institutions have introduced a new structure known as 'bonus bonds' that effectively turn employees into the bank's creditors. The Swiss bank UBS adopted this structure in 2013 – the bonds are forfeited if the bank's regulatory capital ratio falls below 7.5%.

7. The Interdependence of Organizational Units in Risk Governance

In an organization there are various functional units within a firm that depend on each other when it comes to risk management and reporting. Figure 3.2 from the curriculum illustrates this relationship.



8. Assessing the Bank's Audit Function

A bank's internal auditors report to its audit committee. Internal auditors are responsible for:

- Reviewing risk monitoring procedures
- Tracking the progress of risk management system upgrades
- Affirming the efficacy of the existing policies/systems
- Reviewing documentation related to compliance with stipulated standards
- Evaluating the design and conceptual soundness of risk measurement
- Validating market risk models by back testing investment strategies
- Analyzing assumptions about volatility, correlations, and other parameters used in risk models.

As a basic principle, the bank's audit function should be independent from the underlying activity being audited. If this independence is not maintained, conflict of interest could compromise the quality of both risk management and audit activity.

Summary

LO: Explain changes in regulations and corporate risk governance that occurred as a result of the 2007–2009 financial crisis.

Key lessons learnt from the 2007-2009 financial crisis with respect to corporate governance are:

- Stakeholder priority: Instead of focusing solely on shareholders, all stakeholders' interests should be considered.
- Board composition: Boards should be composed such that they strike the right balance of independence, engagement, and financial industry expertise.
- Board risk oversight: Boards should be more proactive in risk management.
- Risk appetite: Boards should clearly articulate a firm's risk appetite.
- Compensation: Boards should exercise control over compensation schemes to prevent undesired risk taking.

Basel III and Dodd-Frank Act were specific regulations introduced to address these issues.

LO: Describe best practices for the governance of a firm's risk management processes.

The best practices for the governance of a firm's risk management processes are:

- BOD should comprise of a majority of independent members. The CEO and the chairperson of the board should be two different and independent people.
- All board members should possess basic knowledge of the firm's business and industry.
- The board should serve in the best interest of all stakeholders and not just the shareholders.
- BOD should address conflict of interest between the management and shareholders (agency risk) well.
- Management compensation plans should be well designed to keep executives from being tempted to prioritize short-term results over long-term goals.
- Board should also appoint a CRO. The CRO or Chief Risk Officer is the person who helps the board understand the firm's risk mapping and risk management process.

LO: Explain the risk management role and responsibilities of a firm's board of directors.

The board must proactively participate in strategic planning and set up an appropriate risk appetite for the firm.

The board should assess whether any major transaction undertaken by the firm is consistent with the authorized risk and associated business strategies.

The board must ensure that procedures for identifying, assessing, and managing various types of risk (business, operational, liquidity etc.) are in place.

The board should take the decision of whether known risks should be retained, avoided, mitigated or transferred.

The board must evaluate the firm's compensation strategy. Executives should be compensated based on their risk-adjusted performance.

The board should ensure that the information it receives about risk management implementation is accurate and reliable.

The board should consist of a risk committee whose members have enough experience to analyze key risks properly. The board risk committee and audit committee should be two separate entities.

LO: Evaluate the relationship between a firm's risk appetite and its business strategy, including the role of incentives.

A firm's risk appetite should be defined to support the firm's business strategy and should be directly linked to the firm's strategic goals. However, the risk appetite should also reflect its tolerance to accept risk. For example, extending loans to subprime borrowers at high interest rates may be potentially profitable, but it may not fit the bank's risk tolerance limits.

Compensation should be designed such that it incentivizes long-term value creation. It should not have a call option like structure that encourages short-term risk taking.

LO: Illustrate the interdependence of functional units within a firm as it relates to risk management.

In an organization there are various functional units within a firm that depend on each other when it comes to risk management and reporting. Senior management, business line managers, finance and operations departments, and risk management teams all coordinate and work together to execute a firm's risk management objective.

LO: Assess the role and responsibilities of a firm's audit committee.

Internal auditors are responsible for:

- Reviewing risk monitoring procedures
- Tracking the progress of risk management system upgrades
- Affirming the efficacy of the existing policies/systems
- Reviewing documentation related to compliance with stipulated standards
- Evaluating the design and conceptual soundness of risk measurement
- Validating market risk models by back testing investment strategies
- Analyzing assumptions about volatility, correlations, and other parameters used in risk models.

