Chapter 3. The Governance of Risk Management

- **Explain changes in corporate risk governance that occurred as a result of the 2007 — 2009 financial crisis.**
- **Describe best practices for the governance of a firm's risk management processes.**
- **Explain the risk management role and responsibilities of a firm's board of directors.**
- **Evaluate the relationship between a firm's risk appetite and its business strategy, including the role of incentives.**
- **Illustrate the interdependence of functional units within a firm as it relates to risk management.**
- **Assess the role and responsibilities of a firm's audit committee.**

Explain changes in corporate risk governance that occurred as a result of the 2007 — 2009 financial crisis.

Corporate governance refers to the roles, responsibilities, and relationships among the firm's shareholders, board of directors, and senior management.

Prior to the global financial crisis (GFC), risk management was marginalized, as many management teams prioritized growth and higher returns (rather than risk-adjusted returns). The GFC implicated several risk management failures. The proximate trigger was a downturn in the real estate (i.e., housing) market. Mortgage-backed securities (MBS) fuelled loose lending policies; some lenders descended into unsound practices by lending to unqualified individuals. Complex securitizations (e.g., CDOs or even CDOs-squared) rippled the risks into credit markets. The rating agencies failed to identify the risks and often assigned AAA ratings to tranches that contained significant default (not to mention valuation) risk.

Several financial institutions failed. The crisis started in the United States but impacted banking and economic activity across the globe. The GFC is a glaring example of *systemic risk* realized!

The GFC exposed the inadequacy of the corporate governance practices and their associated regulations. More subjectively, most observers lamented a lack of managerial accountability in the context of failures of internal oversight. In this way, the GFC elevated the discussion around corporate governance.

The Basel Committee on Banking Supervision (BCBS) decided to confront these governance failures. In October 2010, BCBS issued principles designed to improve corporate governance. The principles were revised in 2015 and defined the roles of the board and its risk committees, senior management (including the Chief Risk Officer), and internal auditors.

Table 3.2: Corporate governance principles for banks[1]

1.	Board's Overall Responsibilities	The board has overall responsibility for the bank, including approving and overseeing management's implementation of the bank's strategic objectives, governance framework, and corporate culture.
2.	Board Qualifications and Composition	Board members should be (and remain) qualified for their positions. They should understand their oversight and corporate governance role and be able to exercise sound, objective judgment about the affairs of the bank.
3.	Board's Own Structure and Practices	The board should define appropriate governance structures and practices for its own work and put in place the means for such practices to be followed and periodically reviewed for ongoing effectiveness.
4.	Senior Management	Under the direction and oversight of the board, senior management should carry out and manage the bank's activities in a manner consistent with the business strategy, risk appetite, remuneration, and other policies approved by the board.
5.	Governance of Group Structures	In a group structure, the board of the parent firm has the overall responsibility for the group and for ensuring the establishment and operation of a clear governance framework appropriate to the structure, business, and risks of the group and its entities. The board and senior management should know and understand the bank group's organizational structure and the risks that it poses.
6.	Risk Management Function	Banks should have an effective independent risk management function, under the direction of a chief risk officer, with sufficient stature, independence, resources, and access to the board.
7.	Risk Identification, Monitoring, and Controlling	Risks should be identified, monitored, and controlled on an ongoing bank-wide and individual entity basis. The sophistication of the bank's risk management and internal control infrastructure should keep pace with changes to the bank's risk profile, the external risk landscape, and industry practice.
8.	Risk Communication	An effective risk governance framework requires robust communication within the bank about risk, both across the organization and through reporting to the board and senior management.
9.	Compliance	The bank's board of directors oversees the management of the bank's compliance risk. The board should establish a compliance function and approve the bank's policies and processes for identifying, assessing, monitoring, reporting, and advising on compliance risk.
10.	Internal Audit	The internal audit function should provide independent assurance to the board and support the board and senior management in promoting an effective governance process and the long-term soundness of the bank.
11.	Compensation	The bank's remuneration structure should support sound corporate governance and risk management.
12.	Disclosure and Transparency	The governance of the bank should be transparent to its shareholders, depositors, other relevant stakeholders, and market participants.
13.	Role of Supervisors	Supervisors should provide guidance for and supervise corporate governance at banks through comprehensive evaluations and regular interaction with boards and senior management; should require improvement and remedial action as necessary; should share information on corporate governance with other supervisors.

[1] Basel Committee on Banking Supervision, Guidelines: Corporate Governance Principles for Banks, July 2015

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

The board has a duty to shareholders but must also be sensitive to debt holders.

- The board's key responsibility is to protect shareholders' interests.
- Additionally, the board should be concerned about other stakeholders. This includes sources of capital (e.g., debt holders concerned with downside risk) and non-financial stakeholders, especially employees.
- It is the board's job to oversee executive management. The board must watch for any conflicts of interest between management's activity and shareholder welfare, for example, if managers are boosting short-term profits at the expense of long-term shareholder value.

But conflicts of interest (or, less severely, lack of alignment) can easily happen.

- For example, if executives are rewarded with options that they can cash in if the share price of the company rises above a certain level. This gives management an incentive to push the share price up, but not necessarily in a sustainable way. The tension between the interests of the CEO and the interests of longer-term stakeholders helps to explain why boards of directors need to maintain their independence from executive teams and why there is a global push to separate the role of the CEO and the chairman of the board. [2]

  It is difficult (impossible?) to completely separate corporate governance from risk management—good risk management requires good governance.

Many corporations have created the role of chief risk officer (CRO).[2]

- A key duty of the CRO is to act as a senior member of the management committee and to attend board meetings regularly. The board and the management committee look to the CRO to integrate corporate governance responsibilities with the risk function's existing market, credit, operational, and business risk responsibilities.
- After the financial crisis of 2007–2009, many CROs were given a direct reporting line to the board or its risk committees in addition to reporting to the executive team and CEO.

[2] Michel Crouhy, Dan Galai, and Robert Mark, The Essentials of Risk Management, 2nd Ed. (NY: McGraw-Hill, 2014)

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

The board must ensure a clear understanding of the firm's business strategy and the strategy's implied fundamental risks and rewards.

- Oversee, and hold accountable, the executive team
- Ensure transparency by way of adequate internal and external disclosure.
- Contribute to the firm's overall strategic plan. This includes types of risks (and degree of risks) that are acceptable for the firm.
- Ensure the firm has installed an effective risk management program consistent with the firms' articulated strategy and risk appetite. Ensure there exists procedures for identifying, assessing, and managing all types of risk.

The four basic choices in risk management:[3]

- **Avoid risk** by deciding not to carry out certain activities.
- **Transfer risk** to third parties through insurance, hedging, and outsourcing.
- **Mitigate risk** via preventive and detective control methods.
- **Accept risk**, recognizing that undertaking certain risky activities should generate shareholder value.

Some firms create an Ethics Committee to ensure that soft risks (unethical business practices) do not translate into hard risks (e.g., illegal activity).

The modern board must also be proactively alert the firm's *executive compensation plans* and its general incentive plans. History proves people respond to incentives. Compensation should be linked to risk-adjusted performance, which in turn should align with shareholders' interests. The board must be thoughtful about the size and design of equity-based compensation (e.g., executive stock options, aka, ESOs), given they are double-edged swords. Although ESOs align somewhat with shareholders, they can encourage excessive risk-taking. For example, under-water options may expire worthlessly unless the CEO takes a big gamble, like an acquisition.

Board and Committees

- Members of the Risk Committee need technical skills plus solid business experience
- The Risk Committee should be separate from the Audit Committee (which requires different skills)
- At many firms, the primary Committees ratify key policies and procedures. These Committees also ensure the effective implementation of such policies.
- Banks should have a Credit Risk Management Committee. Its role includes credit risk reporting and monitoring credit risk limits.

[3] Michel Crouhy, Dan Galai, and Robert Mark, The Essentials of Risk Management, 2nd Ed. (NY: McGraw-Hill, 2014)

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

The firm's risk appetite should connect to business strategy and capital plans.

- The risk appetite identifies activities that are inappropriate (i.e., too risky) for the firm. Some activities are ill-advised in relation to the firm's balance sheet.
- To articulate the risk appetite, board members need education and the means to explore issues.
- The board should be able to articulate acceptable loss level(s) over a specified time horizon. This is a simple high-level output but requires many non-trivial inputs, including grasping the firm's realistic risk profile, and its culture

A firm must be able to link risk appetite and risk tolerances to limits at the business unit and portfolio level.

- Market risk limits control the risk due to changes in the absolute asset price.
- Credit risk limits manage the number of defaults and downward migration in the portfolio's credit quality. For illiquid products, the firm should set tight limits on exposure concerning asset/liability management risk and market liquidity risk

Limits and limit standards policies[4]

Most institutions employ two types of limits.

- **Type A (tier 1) limits** include a single overall limit for each asset class and a single overall stress test limit plus a cumulative loss from the peak limit. Type A limits for market risk might be set at a level such that the business, in the normal course of its activities and normal markets, has exposures of about 40% to 60% of its limit. Peak usage of limits in normal markets should generate exposures of 85% of the limit.[4]
- **Type B (tier 2) limits** are more general and cover authorized business and concentration limits.

Sophisticated complements

- It is best practice to *complement* traditional limits with more advanced risk metrics such as value-at-risk (VaR) and expected shortfall (ES).
- The caveat is that VaR performs better under "normal market conditions" and for familiar portfolios, but VaR is less reliable under extreme conditions and when the portfolio is specialized.
- Best practice includes complementing both limits and sophisticated measures (e.g., VaR and ES) with scenario analysis and stress testing so that worst-case scenarios are at least contemplated.

[4] Michel Crouhy, Dan Galai, and Robert Mark, The Essentials of Risk Management, 2nd Ed. (NY: McGraw-Hill, 2014)

Standards for Monitoring Risk

Limits must be monitored if they are to be effective.

- Market risk positions should be valued daily, e.g., mark-to-market. Units should provide daily profit and loss (P&L) statements to senior management. All model assumptions should be independently verified.
- The trading team's compliance with risk limits should be routinely reported. When limit exceptions are observed, there should be a timely escalation procedure.
- Actual portfolio volatility should be compared to predicted portfolio volatility. Simulations (and stress tests) should estimate the impact of major variables changes to the P&L.

Role of Incentives

The global financial crisis (GFC) demonstrated that many incentive plans encouraged ill-advised short-term risk-taking. Two problems were short-term bonuses that rewarded managers for annual performance but did not penalize them for the ensuing risks created (risks that might materialize several *years* later) and stock options. Consequently, many regulators now require a formal board Compensation Committee.

A lesson of the GFC is that compensation is a fundamental component of risk culture, and compensation is part of enterprise-wide risk management (ERM). At the same time, revenue-generating individuals (aka, rainmakers) will always be valuable to any firm.

In 2009, the G-20 called on central banks to establish an international framework "to promote financial stability, including a reform of compensation practices." In an endorsement of the FSB's implementation standards, the G-20 recommendations included:

- The elimination of multi-annual guaranteed bonuses;
- The incorporation of executive downside exposure through the deferral of certain compensation, the adoption of share-based remuneration to incentivize long-term value creation, and the introduction of clawback provisions that require reimbursement of bonuses should longer-term losses be incurred after bonuses are paid;
- Limitations on the amount of variable compensation granted to employees relative to total net revenues;
- Disclosure requirements to enhance transparency; and
- Affirming the independence of the committees responsible for executive compensation oversight to ensure their alignment with performance and risk.[5]

In 2014, the FSB reported that the implementation of these standards was essentially complete in almost all FSB jurisdictions. In some jurisdictions (e.g., the European Union), regulators went beyond the recommended standards. They adopted bonus caps equal to 100% of an executive's salary or, if approved by two-thirds of shareholders, 200% of their salary.[6]

[5] G20 Leaders Statement: The Pittsburgh Summit, September 24–25, 2009, Pittsburgh http://www.g20.utoronto.ca/2009/2009communique0925.html(accessed 19/4/2018)
[6] GARP (Global Association of Risk Professionals, 2020)

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

Risk Committee of the Board[7]

- At the top of the tree, the board's risk committee approves the bank's risk appetite each year, based on a well-defined and broad set of risk measures (such as the amount of overall interest rate risk).
- Delegates authority to the bank's senior risk committee, chaired by the CEO of the firm, whose membership includes the chief risk officer (CRO), the head of compliance, the heads of the business units, the CFO, and the treasurer.

Senior Risk Committee[7]

- Recommends to the Risk Committee of the Board an amount at risk that it is prudent for their approval
- Determines the amount of financial and non-financial risk to be assumed by the bank as a whole, in line with the bank's business strategies.
- Responsible for establishing, documenting, and enforcing all policies that involve risk and for delegating specific business-level risk limits to the CRO of the bank. **Delegates to the CRO the authority to make day-to-day decisions on its behalf.** The senior risk committee of the bank reviews in detail and approves each business unit's mandate in terms of their risk limits and delegates the monitoring of these limits to the CRO.

Chief Risk Officer (CRO)[7]

- Responsible for designing the bank's risk management strategy
- Responsible for the risk policies, risk methodologies, risk infrastructure, and corporate risk governance.
- Plays a pivotal role in informing the board and the bank's senior risk committee about the appetite for risk across the bank.
- Communicates the views of the board and senior management down through the organization.
- Responsible for independently monitoring the limits throughout the year.
- May order business units to reduce their positions or close them out because of concerns about market, credit, or operational risks.
- Delegates some responsibilities to the heads of the various business units.

[7] Michel Crouhy, Dan Galai, and Robert Mark, The Essentials of Risk Management, 2nd Ed. (NY: McGraw-Hill, 2014)

Business risk committee[8]

At the level of each major business, there may also be a business risk committee comprised of both business and risk personnel.

- The focus of the business risk committee is to make sure that business decisions are in line with the corporation's desired risk/reward trade-offs and that risks are managed appropriately at the business line level
- May be responsible for managing business-level design issues that set out how a particular risk will be managed, reflecting the agreed-upon relationship between the business and the bank's risk management function.
- Approves policies that define the appropriate measurement and management of risk and provides a detailed review of risk limits and risk authorities within the business unit.

Key lessons of financial crisis[8]

The financial crisis highlighted the need to re-empower risk officers in financial institutions, particularly at a senior level. The key lessons are:

- CROs should not just be after-the-fact risk managers but also risk strategists; they should play a significant role in determining the risks that the bank assumes and helping to manage those risks.
- To ensure there is a strategic focus on risk management at a high level, the CRO should report to the chief executive officer (CEO) and have a seat on the board's risk management committee.
- The CRO should engage directly, regularly, with the risk committee of the board. The CRO should regularly report to the full board to review risk issues and exposures. A strong independent voice will mean that the CRO will have a mandate to bring to the attention of both line and senior management, or the board, any situation that could materially violate risk appetite guidelines.
- The CRO should be independent of line business management and have a strong enough voice to make a meaningful impact on decisions.
- The CRO must evaluate all new financial products to verify that the expected return is consistent with the risks undertaken and that the risks are consistent with the business strategy of the institution.

[8] Michel Crouhy, Dan Galai, and Robert Mark, The Essentials of Risk Management, 2nd Ed. (NY: McGraw-Hill, 2014)

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

The audit function should provide an independent assessment of the design and implementation of the bank's risk management.

The Audit Committee should evaluate the firm's risk measures (e.g., are they conceptually sound?), and, in particular, internal auditors should validate models via **back-testing**.

Internal auditors should review risk management processes. For *market risk*, this includes the approval process for vetting **valuation** models, the **validation** of material changes to risk measurement protocols, and the **scope** of risks captured by risk models. In general, regulators will require that internal auditors examine management information systems (MIS) and position data concerning its independence, accuracy, and completeness.

- Audit is also responsible for controls over market position data capture and the parameter estimation processes.
- Provides assurance with respect to databases that inform parameters into market VaR and credit VaR analytics.
- Adequacy of risk monitoring procedures, system upgrades, and adequacy of application controls.
- Documentation relating to compliance with the criteria (qualitative and quantitative) required by any regulatory guidelines.