3. The Governance of Risk Management

FRM Part 1: Foundations of Risk Management

Devere Anthony Weaver

---

1 Corporate Governance

Corporate governance is the way in which companies are run. It describes the roles and responsibilities of a firm's shareholders, board of directors, and senior management.

---

2 Sarbanes-Oxley Act of 2002 (SOX)

The overall goal of SOX was to impose strict financial reporting and auditing parameters on public companies.

The practical implication of SOX include:

- CEOs and CFOs must personally verify and certify the ac curacies of financial findings with the SEC
- CEOs and CFOs must attest that company disclosures provide and accurate picture of the firm
- Certain internal controls are required and any deficiencies must be reported to regulators immediately
- Reporting and internal controls must be reported annually
- The names of individuals who serve on the board audit committee are to be disclosed
- The individuals on the board audit committee and expected to understand accounting principles, be able to comprehend financial statements, and have experience with internal audits and understand the functions of the audit committee

---

3 The Post-Crisis Regulatory Response

The *Basel Committee on Banking Supervision (BCBS)* is an organization comprised of the central banks and bank supervisors from 27 jurisdictions.

BCBS focused on formalizing international standards for prudential banking regulation. The standard that are set by BCBS are *voluntary* and not legally binding.

3.1 Basel I (1998 Basel Accord

Basel I focused on devising a uniform method for setting capital adequacy standards in the wake of the Latin American debt crises. It was focused primarily on *credit risk*.

The main takeaway is that it introduced a risk-weighted approach to capital requirements by setting the prescribed minimum capital at 8% of a firm's risk-weighted assets.

3.2 Basel II

Basel II introduced trading and lending activities into a firm's capital adequacy standards.

It kept the 8% of risk-weighted credit standards, but it also introduced standards for supervisory bank reviews as well as disclosure requirements to reinforce market discipline through transparency.

3.3 Basel III

Basel III was the direct response to the global financial crisis (GFC) and focused on greater systematic resiliency in the banking system.

Basel III's big change was that it introduced a focus onto both *idiosyncratic risk* (firm-specific) and systemic risk (risk of a failure of a major financial institution causing interconnected financial institutions to fail).

Basel III kept most of the previously implmented regulatory capital standards in place, but it introduced a few more factors to help limit risk:

- raises capital quality by limiting core Tier 1 capital to common equity and retained earnings, this provides lost absorption unlike other hybrid debt
  - *tier 1 capital* is the primary capital a firm needs to conduct its business operations to remain solvent; it is the sum of *common stock, retained earnings* and certain reserves.
- imposes new short-term liquidity funding ratios where banks must hold enough highly liquid assets to fund 30 worth of cash needs
- imposes new long-term funding ratios where banks must hold at least 1 year's worth of stable cash flow to fund required operations
- designed *macroprudential* regulation that is intended to reduce overall systemic risk consisting of the following 5 elements:
  1. a leverage ratio cap of 3% (the leverage ratio measures debt relative to some other metric, *but why is this important?...*)
  2. introduces a countercyclical capital buffer
     - "A countercyclical capital buffer would raise banks' capital requirements during economic expansions, with banks required to maintain a higher capital-to-asset ratio when the economy is performing well and loan volumes are growing rapidly. Conversely, it would require a lower capital-to-asset ratio during recessions"
  3. set a minimum total loss-absorbing capital (TLAC) standards that apply to glocal systematically important banks
  4. encouraging as many trades as possible to be centrally cleared, as opposed to trades being done in OTC markets
  5. modifying risk modeling and stress testing to better capture tail risk events

Basel III also revised a framework for handling market risk by introducing the *Fundamental Review of the Trading Book (FRTB)*. FRTB is designed to focus on risk introduced through a bank's trading desk in derivatives, futures, and other complex financial assets.

3.4 Dodd-Frank Act

Prior to 1999, commercial and investment banks were segregated under the Glass-Steagall act in the 1920s. In 1999, the Graham-Leach-Bliley Act enabled bank holding companies to convert into *financial services holding companies (FSHCs)* that could combine investment banking, commercial banking, insurance, and brokerage activities under one corporate umbrella.

Unfortunately, all these activities conducted by one corporation led to some massive oversights (unintentional or not), culminating in the GFC.

In 2010, the *Dodd-Frank Act* was signed into law to address the following key elements:

1. strengthening of the Fed - the Fed was given oversight of all systematically important financial institutions (SIFIs), these are defined as holding firms with over $50 billion USD worth of assets.

2. ending to big to fail - the act ended too big to fail by creating an orderly liquidation authority (OLA) that would liquidate failing holding companies
3. resolution plan - SIFI's are now required to submit a "living will" to the Fed and FDIC that lays our a corporate governance structure for resolution planning
4. derivatives markets - newly implemented overhaul of the derivatives market to allow for more transparency to help with counterparty risk
5. Volcker rule - imposes prohibition on proprietary trading by public institutions
6. consumer protection - the creation of the Consumer Financial Protection Bureau (CFPB) to regulate consumer financial services
7. stress testing - instituted a new approach to scenario analysis and stress testing conducted by the Fed:
    - The *Dodd-Frank Act Stress Test (DFAST)* for banks with assets above $10 billion USD
    - The *Comprehensive Capital Analysis and Review (CCAR)* for banks with assets above $50 billion USD

3.4.1 European Regulatory Response

European regulators introduced the *Supervisory Review and Evaluation Process (SREP)*; however, it's not a stringent as the American response to the crisis.

---

4 Infrastructure of Risk Governance

The board of directors is responsible for overseeing the analysis of risk and returns from corporate activity. It must also manage conflicts of interest between the shareholders and management.

Basically, when it comes to corporate governance issues, the board of directors is in charge and ultimately responsible for when a risk policy is ignored or violated.

To do this, the board should have a risk committee whose members have enough analytic sophistication and business experience to properly analyze key risks.

---

5 Risk Appetite Statement

Publishing a risk appetite statement (RAS) is a major component of corporate governance.

A RAS is a "written articulation of the aggregate level and types of risk that firm will accept or avoid in order to achieve its business objectives".

It's important to note that the RAS includes both *quantitative* and *qualitative* statements of risk. Quantitative statements of risk give an actual numerical measure about the risk a company is willing to take. The qualitative statements are statements that outright say what risks the firm is willing to take (or not) without any measurement.

Risk tolerance refers to the *range* of acceptable outcomes related to achieving a business objective. It is a tactical measure whereas our risk appetite is a broad aggregate measures of the amount at risk.

Again, we'll typically want to set the risk appetite at a level sufficiently below the risk capacity to ensure that the actual risk stays well below the risk capacity of the firm.

Doing so keeps the risk profile within the risk tolerance bands to provide comfort we can achieve the desired risk-adjusted return objectives subject to limiting the amount of risk.

---

6 Implementing Board-Level Risk Governance

6.1 The Board Audit Committee

An effective audit committee is essential to the director's oversight of the firm.

The board audit committee is responsible for the accuracy and completeness of a firm's financial and regulatory disclosures. It is also responsible for ensuring compliance with best practice standards in non-financial matters.

6.2 Risk Advisory Director

The risk advisory directory is a board member that intimately understands risk factors of a given industry and can advise the board on specialized risk exposures.

6.3 Risk Management Committee

Is responsible for setting the firm's risk appetite and independently monitoring ongoing risk management. They also provide supervision of known risks, approve high-level risk decisions, and approve credit facilities and limits.

6.4 Compensation Committee

Is responsible for the discussion and approval of enumeration of key management personnel.

---

7 Organizational Units in Risk Governance

Risk management implementation is the primary responsibility of the firm's staff.

Executive and business line managers work together to manage, monitor, and report various types risk being undertaken. They also are needed for the verification of timely, accurate, and completed deal capture and affirmation of official P&L statements.

A bank's *operation function* plays a critical role in risk oversight. This unit can independently execute, record, and settle trades; reconcile positions, and chronicle all transactions.

The finance group is responsible for developing valuation and finance policies.