Lecture

IAQS | INSTITUTE OF ACTUARIAL & QUANTITATIVE STUDIES

Class: TY BSc

Subject : Risk Management & Investment Management -1

Subject Code: PUSASQF5.

Chapter: Unit 2 Chp 1

Chapter Name: Enterprise Risk Management - Introduction

We previously learned

- M&M analysis and CAPM are important theoretical arguments against risk management. But they function on the assumption that capital markets are perfect, which we hardly see in practice. Those opposed also point out that risk management is a zero-sum game and can be detrimental when implemented wrongly.
- Risk management in practice though smoothens cash flow and reduces cost of capital and compliance for the firm. It also helps set up a risk appetite and enhances the ability of firms to finance growth while communicating well with the shareholders about objectives.
- Firms can broadly use four different strategies to manage risks, namely; Accept the risk, Avoid the risk, Mitigate risk & Transfer the risk.
- After getting an idea of the strategies that can be used, the firms should put risk management into practice. The first step involves determining the objective of the risk management policy of the firm.
- A independent Board of Directors is necessary for formulating a good risk management policy and how the board is constituted is crucial. The BoD formulates the strategy and conveys risk appetite of the firm and how to manage it.
- Risk appetite refers to the level (and types) of risk that a firm is willing to retain. Risk willingness relates to a firm's desire to accept risk in pursuit of its business goals, while risk ability can put a cap on risk willingness for various reasons.
- After a firm establishes its risk appetite, it should assemble an inventory of all known risks. This process is called risk mapping.

Continued…

- After a risk appetite is established and risks mapped, hedging is undertaken according to the needs of the firm. Hedging is essentially insuring the firm against various negative events and can be undertaken in various forms.
- Pricing risk, Foreign Currency risk and Interest-rate risk are the significant business and financial risks to be hedged against. By making the realistic assumption that there are some imperfections in the financial markets, a firm could benefit from hedging financial risk.
- Hedging activities should cover both the firm's assets and liabilities to fully account for the risks. A dynamic or a static hedging strategy can be used depending on the expertise available and the risks faced by the firm.
- There are various instruments available to manage risks, namely; Forwards and Futures contracts, Call and Put options, Swap and Swaption contracts, Exotic options and Credit Derivatives.
- A well calibrated and executed risk management strategy can lower the risks for the firm while also allowing it to use it as a growth opportunity. The limits and complexity of using these instruments should be understood well before using them.

Topics to be covered

1. Enterprise Risk Management (ERM)
    1. Definitions
    2. Framework

2. Costs and Benefits of ERM
    1. Benefits
    2. Costs
    3. Motivation to adopt ERM

3. Chief Risk Officer (CRO)
    1. Role
    2. Responsibilities
    3. Interaction with other senior management

Continued…

4. Risk Governance
    1. Risk Advisory Director
    2. Risk Management Committee
    3. Compensation Committee
    4. Audit Committee

5. Components of ERM

6. Risk Culture
    1. Indicators
    2. Other factors

1 Enterprise Risk Management (ERM)

Definitions

Enterprise risk management is a process, effected by an entity's board of directors, management, and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.

-Committee of Sponsoring Organizations of the Treadway Commission (COSO), 2004

Risk is the "effect of uncertainty on objectives" and risk management refers to "coordinated activities to direct and control an organization with regard to risk."

-International Organization of Standardization (ISO 31000)

So as we can see, there are different perceptions and hence definitions of risk & risk management. The practice of ERM is relatively new and hence there is no widely accepted industry standard or definition regarding it.

1 Enterprise Risk Management (ERM)

- The lack of a standard ERM definition can cause confusion for a company looking to set up an ERM framework. No ERM definition is perfect or applicable to every organization.
- Therefore each organization should adopt an ERM definition and framework that best fits their business scope and complexity.
- Some organizations may have a top-down approach towards risk management while others may prefer a bottom-up approach.
- The whole ERM framework though should focus around integration of risk management and hence a central risk management unit.

1 Enterprise Risk Management (ERM)

Framework

Though some common themes and points should be kept in mind while making a framework:

i. There should be board involvement in ERM.
ii. ERM is a component of a company's strategy.
iii. It involves identifying potential adverse events.
iv. As part of ERM the company must identify its risk appetite and manage risks in a way that is consistent with that appetite.
v. ERM should help a company achieve its objectives and be a core part of strategic planning and strategic execution processes.

2 Costs and Benefits of ERM

Benefits

- The major benefits of having an ERM program are:

i. **Increased organizational effectiveness :**
   - It allows managers to focus on the largest threats to the firm rather than day-to-day threats to specific units and business lines. Managers understand crossover risks and as well as correlations between specific risk types better with ERM.

ii. **Better risk reporting :**
   - ERM defines the risk appetite of the entire enterprise and helps firms adhere to the constraints put on risk. It supports regulatory compliance while emerging risks, such as cyber threats, reputation risks, and anti-money laundering (AML) risks, are better managed at the enterprise level.

iii. **Improved business performance :**
   - Total costs of transferring risks (i.e., an optimization of risk transfer expenses) in line with the scale of various risks are better managed through ERM. Risk is incorporated into business model selection and the strategic decisions of the bank. ERM is reassuring to stockholders and other stakeholders of the financial institution.

2 Costs and Benefits of ERM

Costs

- Costs are divided into two categories:

i. **Non-recurring (one-time or start-up) costs :**
   - Consultancy costs for setting up an ERM program.
   - Hardware and software purchases.
   - Training of in-house personnel.

ii. **Recurring (ongoing) costs :**
   - Salaries & benefits of risk management staff.
   - Hardware maintenance & upgrades and software license fees.
   - Spend on instruments used to hedge or manage risks.

2 Costs and Benefits of ERM

Motivation to adopt ERM

- Leading organizations make rational investments in risk management and are proactive, optimizing their risk profiles. These investments are more than offset by improved efficiency and reduced losses.
- Rather than the defensive or control-oriented approaches used to manage downside risk and earnings volatility, ERM optimizes business performance by supporting and influencing pricing, resource allocation and other business decisions. It is during this stage that risk management becomes an offensive weapon for management.
- In the business world, managers are often galvanized into action after a near miss-either a disaster averted within their own organization or an actual crisis at a similar organization. The senior management often takes action in response and are goaded by the regulators towards similar action and goals.

3 Chief Risk Officer (CRO)

Role

- Given that ERM is still a relatively new field, many of the details have yet to be smoothed out of the CRO role.
- There are still substantial ambiguities with regards to where the CRO stands in hierarchy between the board of directors and other executives, namely the CEO, CFO and COO. Mostly the CRO reports to the CFO or CEO but this can lead to friction and clashes.
- Though differing through various organizations, broadly, the CRO is the head of an independent risk function in an organization.

3 Chief Risk Officer (CRO)

Responsibilities

- The typical responsibilities for the office of a CRO are :
  - Providing the overall leadership, vision, and direction for ERM.
  - Establishing an integrated risk management framework for all aspects of risks across the organization.
  - Developing risk management policies, including the quantification of the firm's risk appetite through the specific risk limits.
  - Implementing a set of risk indicators and reports, including losses and incidents, key risk exposures and early warning indicators.
  - Allocation of economic capital to business activities based on risk and optimizing the company's risk portfolio through business activities and risk transfer strategies.
  - Communicating the company's risk profile to key stakeholders such as the board of directors, regulators, stock analysts, rating agencies and business partners.
  - Developing the analytical , systems and data management capabilities to support the risk management program.

3 Chief Risk Officer (CRO)

Interaction with other senior management

- As discussed earlier, there is significant ambivalence regarding the exact role of a CRO and where he stands in an organizational structure compared to the other executives. Nonetheless, the CRO, most importantly should be independent.
- The Board of Directors, as discussed earlier is a body comprising professionals who aren't involved in the day to day functioning of the organization. They appoint the CRO and interact with him on a consistent and reasonable frequency.
- Establishing a dotted-line reporting relationship between the CRO and the board helps smoothen the friction between the CRO and the CEO.
- Under extreme circumstances, that dotted line may convert to a solid line so that the CRO can go directly to the board without fear for his or her job security or compensation. A direct communication channel to the board is one way to ensure that the CRO is independent.
- The CRO also interacts with the audit & compensation committees and increasingly, the risk management committee, to form execution plans and keeps an eye on compliance.

4 Risk Governance

- We've earlier discussed the importance of establishing a board of directors with independent members. They are crucial to the risk governance structure of an organization.
- The board also needs to make sure that risks are made transparent to managers and to stakeholders through adequate internal and external disclosure.
- To fulfill its risk governance responsibilities, the board must ensure that the bank has put in place an effective risk management program that is consistent with these fundamental strategic and risk appetite choices. And it must make sure that there are effective procedures in place for identifying, assessing, and managing all types of risk.
- The board should ensure that business and risk management strategies are directed at economic rather than accounting performance.
- The duty of the board is not, however, to undertake risk management on a day-to-day basis, but to make sure that all the mechanisms used to delegate and drive risk management decisions are functioning properly.
- Alongside the CRO, the risk management and audit committees are important regarding the risk function in an organization.

4 Risk Governance

Risk Advisory Director

- Sometimes, a firm's board can include many individuals with experience from outside the firm's industry. When this happens, it is recommended to have **an independent risk advisory director — a board member who intimately understands the risk factors of a given industry and can advise the board on specialized risk exposures.**
- This individual should attend risk committee and audit committee meetings to provide industry-specific guidance. The risk advisory director also meets with senior management on a regular basis and could be viewed as a liaison between the board and management. Overall, the role involves educating members on best practices in both corporate governance and risk management.

4 Risk Governance

Risk Management Committee

- **The risk management committee (a subset of the full board of directors) is responsible for setting the firm's risk appetite and independently monitoring ongoing risk management.**
- Members will maintain contact with both internal and external auditors to ensure compliance with all relevant policies (e.g., regulations and internal risk limits).
- This committee is also charged with supervision of all known risks of the firm and approving high-level risk decisions. In a banking context, they would be involved with approving credit facilities that are above certain limits or within limits but above a specific threshold.

4 Risk Governance

Compensation Committee

- The existence of agency risk necessitates the board to implement a compensation committee to ensure appropriate risk taking in relation to the long-term risks assumed.
- **The compensation committee is independent of management. Its role is to discuss and approve the remuneration of key management personnel.**
- Management compensation above base salary should be congruent with the goals of the other stakeholders. In that regard, the committee should avoid designing compensation plans (e.g., stock-based compensation) with bonuses based on short-term profits or revenues, given the relative ease in which management may manipulate those amounts.

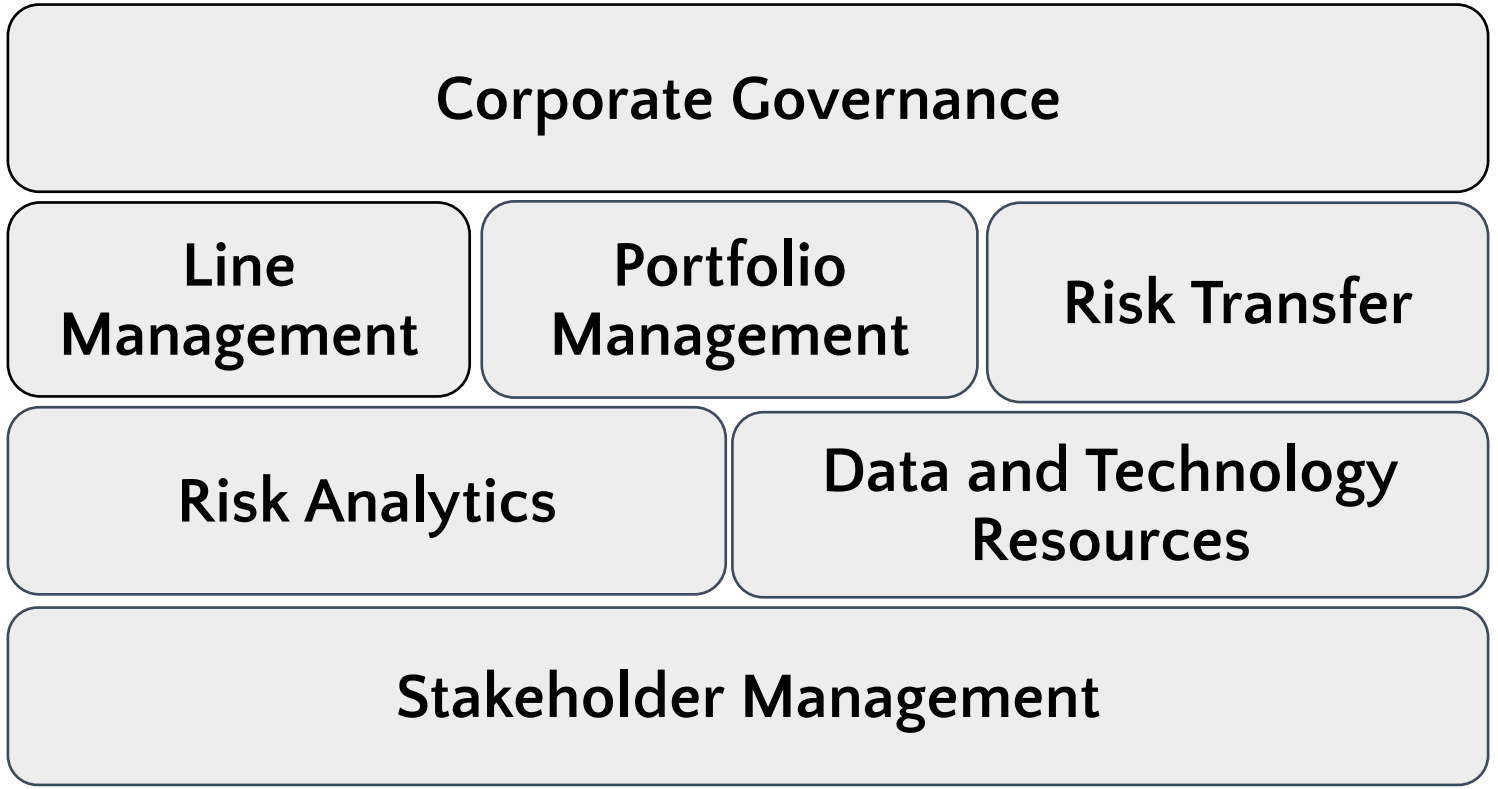
4 Risk Governance

Audit Committee

- The audit committee (a subcommittee of the full board) has traditionally been responsible for the reasonable accuracy of the firm's financial statements and its regulatory reporting requirements.
- The firm's internal auditors report to the audit committee and **they are responsible for monitoring risk management procedures, tracking the progress of existing systems, and affirming the efficacy of the existing policies/systems.**
- The internal auditors should also verify adherence to compliance standards and offer an opinion on the validity of calculated risk metrics like VaR. When market risk is involved, the audit function should validate any pricing models (e.g., derivatives valuation) used for risk monitoring.
- Another key role is to offer an opinion on the assumptions (i.e., volatility, correlations, etc.) used in internal risk estimation.

5 Components of ERM

- The following are the core components of a general ERM program :



5 Components of ERM

- The components must be developed and linked to work as an integrated whole in the following way:
  - **i.** **Corporate governance** to ensure that the board of directors and management have established the appropriate organizational processes and corporate controls to measure and manage risk across the company.
  - **ii.** **Link management** to integrate risk management into the revenue-generating activities of the company (including business development, pricing and so on).
  - **iii.** **Portfolio management** to aggregate risk exposures, incorporate diversification effects and monitor risk concentrations against established risk limits.
  - **iv.** **Risk transfer** to mitigate risk exposures that are deemed too high or are more cost-effective to transfer out to a third party than to hold in the company's risk portfolio.
  - **v.** **Risk analytics** to provide the risk measurement, analysis and reporting tools to quantify the company's risk exposures as well as track external drivers.
  - **vi.** **Data and technology resources** to support the analytics and reporting processes.
  - **vii.** **Stakeholder management** to communicate and report the company's risk information to its key stakeholders.

6 Risk Culture

The risk culture of a firm is the goals, customs, values, and beliefs (both implicit and explicit) that influence the behaviors of employees.

- Establishing a strong risk culture is difficult because it is multilayered. Individuals have their own risk attitudes when they come to work for a firm. Demographics, family backgrounds and experiences, personalities, and professional codes and standards all influence an individual's risk appetite. Peers, as well as management, also influence the risk behaviors of employees.
- Risk culture happens at the enterprise level, the group level (e.g., group think, recruitment of individuals who think like the group), and the individual level.

6 Risk Culture

Indicators

- Firms need methods to measure progress in terms of risk culture. One method is to identify the key risk culture indicators of the firm. The Financial Stability Board (FSB) has specified four risk indicators:
  - **i.** **Tone from the top of the organization :** Are the actions of management in conflict with stated risk goals/appetites? Do compensation plans support the values of the firm or encourage risk-taking? How does the board of directors communicate the fit between risk appetite and firm strategies and goals?
  - **ii.** **Effective communication and challenge :** Are opposing views valued? Are there assessments of managements' "openness to dissent?" Is there stature associated with risk management (or just with performance)?
  - **iii.** **Incentives :** Are compensation plans supportive of and in alignment with risk appetite/risk culture?
  - **iv.** **Accountability :** Are expectations clear? Are escalation processes used?

6 Risk Culture

Other factors

- Other factors that can be used to build a strong risk culture include the following:
  - Knowledge of the firm's risk appetite.
  - Risk literacy
  - The flow of risk information.
  - Risk/reward decisions of managers.
  - Risk management stature.
  - Whistleblowing and escalation.
  - Priorities of the board.
  - Action against offenders.
  - Identification of risk culture concerns/incidents.

Question 1

The basis of enterprise risk management (ERM) is that _____

a) risks are managed within each risk unit but centralized at the senior management level.
b) the silo approach to risk management is the optimal risk management strategy.
c) risks should be managed and centralized within each business or risk unit.
d) it is necessary to appoint a chief risk officer to oversee most risks.

Question 2

Which of the following is not a major benefit of an ERM program?

a) Increased organizational effectiveness.
b) Better risk reporting.
c) Elimination of all risk.
d) Improved business performance.

Question 3

Alex John is a risk analyst at a mid-sized financial institution. He has recently come across an article that described the enterprise risk management (ERM) process. John does not believe this is a well-written article, and he identified four statements that he thinks are incorrect. Which of the following statements identified by John is actually correct?

a) One of the drawbacks of a fully centralized ERM process is overhedging risks and taking out excessive insurance coverage.
b) ERM benefits include better management of risks at the business level, improved business performance, and better risk reporting.
c) ERM uses sensitivity analysis instead of scenario analysis to analyze potential threats.
d) A strong ERM program allows a firm to focus on the largest risks facing the enterprise.

Question 4

It is not the Board of Director's duty to _____

a) make sure that there are effective procedures in place for identifying, assessing, and managing all types of risk.
b) ensure that business and risk management strategies are directed at economic rather than accounting performance.
c) undertake risk management on a day-to-day basis.
d) make sure that risks are made transparent to managers and to stakeholders through adequate internal and external disclosure.

Question 5

The role of a risk advisory director is to _____

a) lead the compensation committee.
b) assume responsibility for setting the enterprise-level risk appetite.
c) provide advice to the executive team of the company.
d) provide risk-oriented expertise to the board when it is primarily comprised of people from industries unrelated to the subject firm.

Question 6

Which of the following statements regarding the role of the firm's audit committee is most accurate?

a) At least one member of the audit committee must possess sufficient financial knowledge.
b) The audit committee may consist of some members of the management team.
c) The audit committee is only responsible for the accuracy of the financial statements.
d) The audit committee is meant to work independently with management.

Question 7

The _____ appoint/appoints the CRO of a firm.

a) Risk Committee
b) CEO
c) Audit Committee
d) Board of Directors

Question 8

Which of the following is not a component of an ERM program?

a) Risk analytics.
b) Risk Transfer.
c) Portfolio Management.
d) Stakeholder Management.
e) None

Question 9

Allen Richards sits on the board of directors of a Canadian financial institution. Richards read the following statements in a presentation made to the board of directors by management on the institution's risk culture:

Statement 1: "As long as managers at business-line levels have the same risk appetite as the overall firm, the risk tolerance of the business-line employees is irrelevant."

Statement 2: "Hiring a chief risk officer will fix the risk culture problems we face at this institution."

Richards believes both of these statements are incorrect. Richards's assessment is accurate with respect to

a) statement 1 only.
b) statement 2 only.
c) both statements.
d) neither statement.

Quick Recap

- The whole Enterprise Risk Management (ERM) framework though should focus around integration of risk management and hence a central risk management unit.
- The major benefits of having an ERM program are : Increased organizational effectiveness , Better risk reporting and Improved business performance.
- Costs for ERM programs can be broadly divided into two categories, recurring and non-recurring or one-time costs.
- Organizations that make rational investments in risk management and are proactive, optimize their risk profiles. These investments are more than offset by improved efficiency and reduced losses.
- The Chief Risk Officer (CRO) is the head of an independent risk function in an organization.
- The CRO is tasked with providing the overall leadership, vision, and direction for ERM, establishing an integrated risk management framework for all aspects of risks across the organization while also communicating with senior management and other stakeholders of the organization.
- The CRO interacts with the Board of Directors on a consistent basis. Establishing a dotted-line reporting relationship between the CRO and the board helps smoothen the friction between the CRO and the CEO.
- The CRO also interacts with the audit & compensation committees and increasingly, the risk management committee, to form execution plans and keeps an eye on compliance.

Continued ...

- The duty of the board is to make sure that all the mechanisms used to delegate and drive risk management decisions are functioning properly.
- An independent risk advisory director is a board member who intimately understands the risk factors of a given industry and can advise the board on specialized risk exposures. The role involves educating members on best practices in both corporate governance and risk management.
- The risk management committee (a subset of the full board of directors) is responsible for setting the firm's risk appetite and independently monitoring ongoing risk management.
- The compensation committee is independent of management. Its role is to discuss and approve the remuneration of key management personnel.
- Audit committee is responsible for monitoring risk management procedures, tracking the progress of existing systems, and affirming the efficacy of the existing policies/systems.
- The core components of an ERM program include Corporate Governance, Line Management, Portfolio Management, Risk Transfer, Risk Analytics, Data and Technology Resources and Stakeholder Management.
- The risk culture of a firm is the goals, customs, values, and beliefs (both implicit and explicit) that influence the behaviors of employees.
- The Financial Stability Board (FSB) has specified four culture risk indicators : Tone from the top of the organization, effective communication and challenge, incentives and accountability.