

Enterprise Risk Management

PMG 611

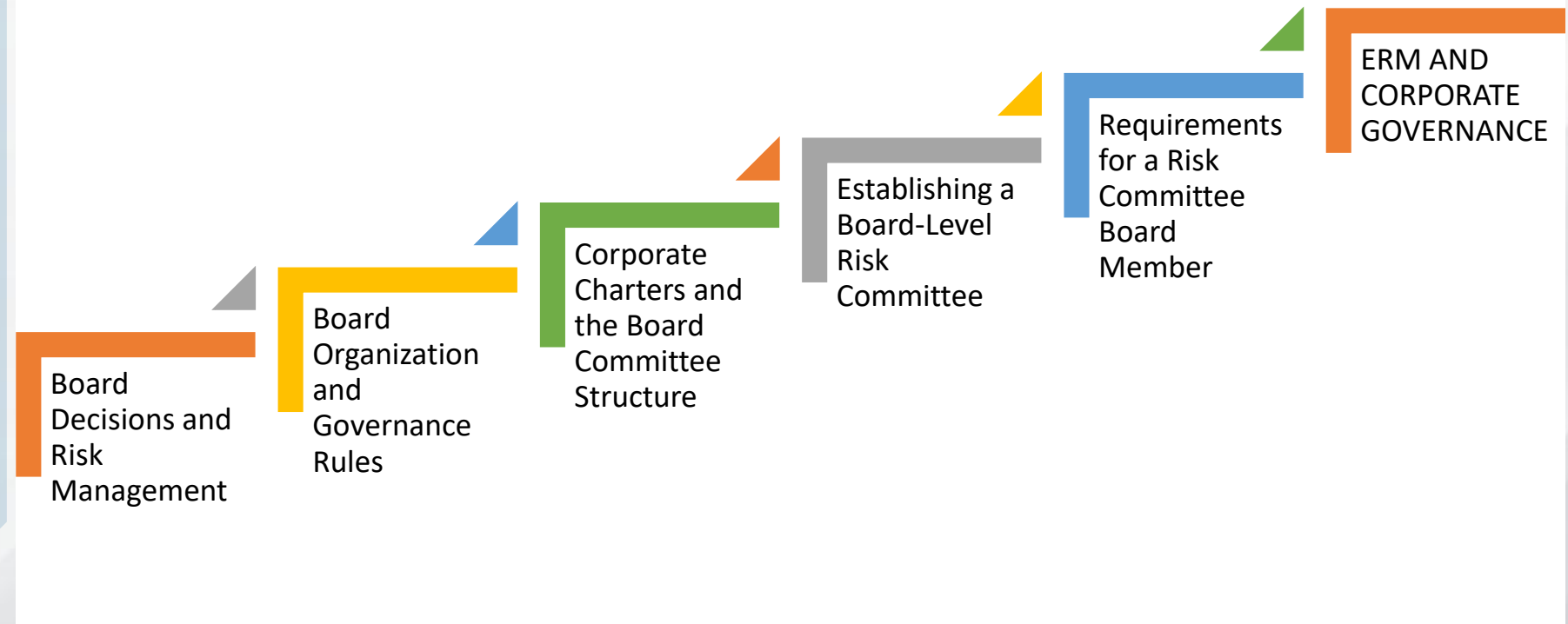
Lecture 8

**Importance of GRC Principles in
the Board Room**

Prepared by
Dr. Eng. Abdullah Jameel Halawany

Lecture
08

Session Outline



Introduction

Lecture

08

Importance of GRC
Principles in the Board
Room

PMG 611
Enterprise Risk Management

Lecture

08

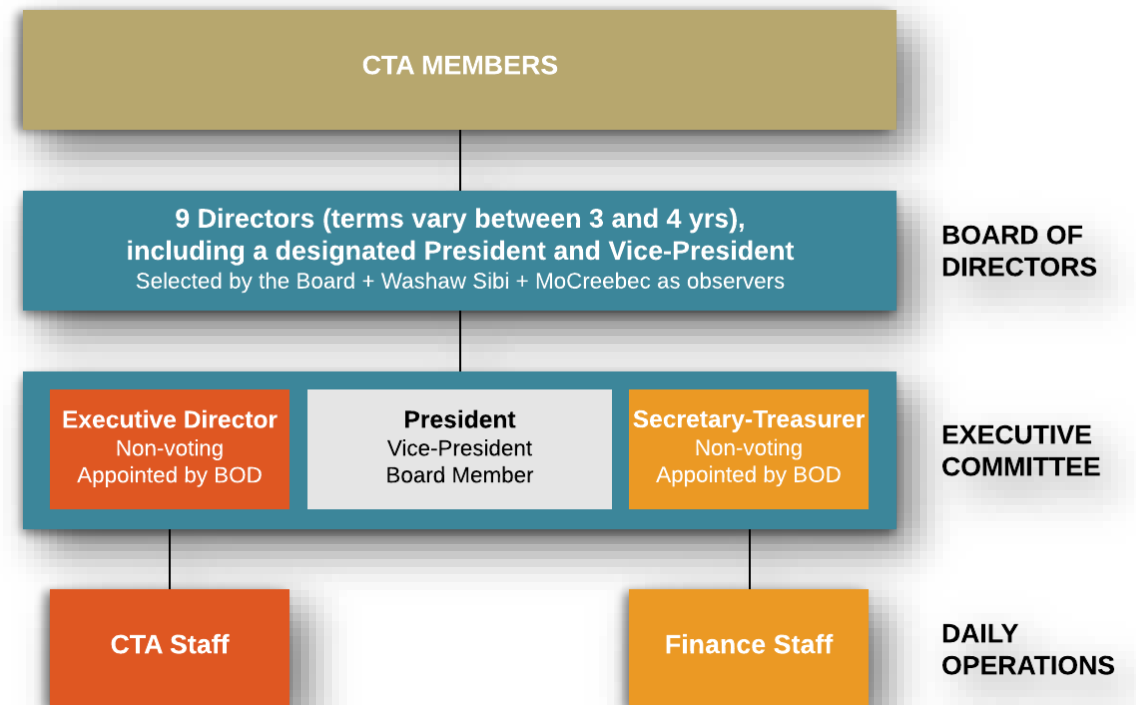
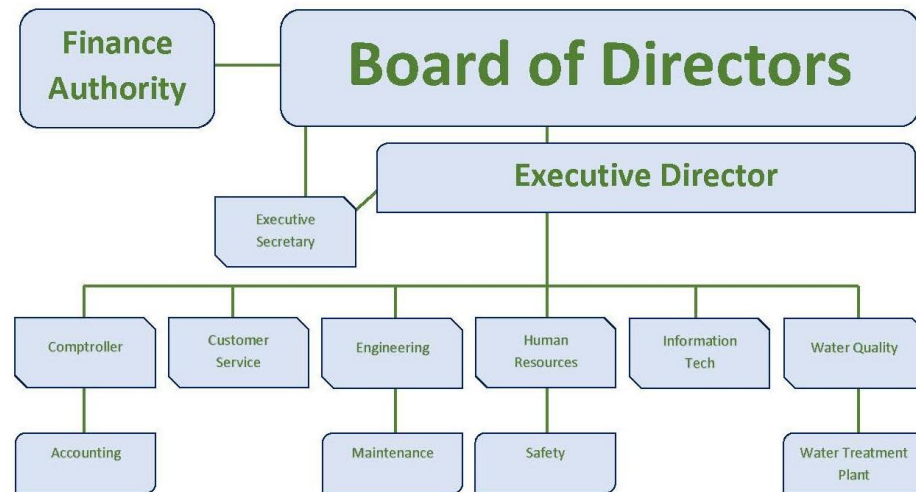
Introduction

- ***The Board Of Directors*** is the ultimate manager of all stockholders in investor-owned enterprises as well as for most large private enterprises.
- Directors may be either elected from the existing stockholders, known as outside or nonemployee directors, or may be directors who are also very senior members of an enterprise's management, called inside or employee directors.
- Charged with independently reviewing and approving all major decisions for the enterprises they manage and serve.

- ***The Board Of Directors*** are the independent managing representatives for the stockholders, with a responsibility to ***make major decisions*** for the corporation based on ***their assessment of the risks*** and ***potential benefits*** presented to them.
- ***Enterprise Risk Management (ERM)*** framework provides an important approach and methodology for the board of directors to assess risks and to make better decisions for an enterprise and its shareholder owners.

Lecture
08

Introduction



Lecture

08

Introduction

- Many CEOs are strong and powerful people with influence and persuasive powers that can heavily influence other board members.
- However, the board can overrule the CEO and can just as easily terminate the services of a CEO or some other senior officer and take actions to bring in someone new.

Lecture

08

Introduction

- Some corporations have both a separate CEO and a chair of the board, two powerful leaders who should work closely together for the greater good of the corporation.
- In other cases, one leader holds the joint chair of the board and CEO titles.
- The trend today is perhaps for two separate chair of the board and CEO leaders.

Board Decisions and Risk Management

Lecture

08

Importance of GRC
Principles in the Board
Room

PMG 611
Enterprise Risk Management

Lecture
08

Board Decisions And Risk Management

- **Board Members** usually are not involved in such daily, full-time work-week activities.
- Will serve on multiple committees beyond the formal full board meetings
- Responsible for reviewing and understanding often massive amounts of financial, operational, and other reports concerning the enterprise they are managing.

Lecture
08

Board Decisions And Risk Management

- Board **Decisions** and the **directions** can have important impacts on the overall enterprise.
- For example, based on good financial results and a strong balance sheet, the board can declare an extra or increased cash dividend.
- The board can also make decisions that are not made with management's full concurrence. (decision goes against that CEO's wishes)

Lecture
08

Board Decisions And Risk Management

- The understanding, evaluation, and acceptance of risk should be a major consideration in almost every board decision.
- Because of their most senior positions in enterprises, board members are expected by many outside of the boardroom—investors, regulators, and others—to have a strong understanding of their corporation and the risks it faces.

Lecture

08

Board Decisions And Risk Management

- Directors should have a good understanding of many of the specific risks that their companies face, such as *risks associated with introducing a new product* into a very competitive marketing environment or of committing capital into a volatile area with the possibility of high rewards.
- As part of good management practices, directors are expected to have a good understanding of managing a wide range of enterprise-level risks.

Lecture
08

Board Decisions And Risk Management

- While directors must comply with financial and accounting regulations, there are no specific rules or requirements for the director-level management and understanding of risks.
- ERM has provided a framework for understanding these risks, but traditionally directors often have no specific guidance or rules covering their acceptance and understanding of dealing with risks.

Lecture
08

Board Decisions And Risk Management

- The most major concept of ERM is this emphasis of enterprise-wide risk management, the very decision area that impacts a corporate director.
- ERM calls for the manager to think of and deal with these risks on a larger, wider plane.
- Just as a manufacturing manager should think of enterprise risks on a wider horizon, ***a corporation director must always have this “big picture” concept of enterprise-wide risks in mind when making nearly all decisions.***

Lecture
08

Board Decisions And Risk Management

- Board members must always keep in mind that their decisions usually cover a wide spectrum.
- Closing a plant, for example, can present **logistics risks** in adjusting or moving people and equipment to sustain operations, **legal risks** associated with various plant closings, **notification risks**, and **public relations risks** in appropriately communicating the closure plans.
- ***Enterprise risk management is a very important board of director-level concept.***

Lecture
08

Board Decisions And Risk Management

- An overall objective here is to ***promote good GRC principles on a board of directors' level.***
- The first - **Governance** - deals with understanding and communicating the rules. (This is and has been an ongoing board requirement).
- Similarly, **Compliance** is a board requirement that deals with following both internal and external rules and procedures. Board members have a personal and professional legal responsibility here.
- ***The R or risk portions of GRC can cause greater challenges at the board level.***

Lecture
08

Board Decisions And Risk Management

- Recent research indicates that many directors of major corporations today **do** **not** always seem to have a good understanding of overall risk management and of the concepts of ERM standards.
- **Board Of Directors** in enterprise-wide risk oversight has become increasingly **challenging** as expectations for board engagement are at an all-time high.

Board Organization and Governance Rules

Lecture

08

Importance of GRC
Principles in the Board
Room

PMG 611
Enterprise Risk Management

Lecture
08

Board Organization And Governance Rules

- Employees working for a corporation are accustomed to following a fairly structured set of enterprise rules and procedures, no matter their employment level or position in an enterprise.
- All are expected to follow their corporate code of conduct guidelines, to generally tailor their work hours to normal operating procedures, and to follow enterprise policies and procedures.
- *These are their corporate and legal rules.*

Lecture

08

Board Organization And Governance Rules

- Other employee practice guidelines are also defined through various professional standards or labor related bargaining unit agreements.
- Some of these rules or standards may apply to all employees while others are very specific.
- Beyond legal and corporate policy rules, enterprise stakeholders are expected to follow a wide range of good practice general guidelines.

Lecture
08

Board Organization And Governance Rules

- Just as every employee, an elected board member also *must follow* a wide range of legal, ethical, and good business practices rules and procedures.
- In addition, because the *board of directors is responsible for the overall governance* of the corporation, the collective board and its individual members are *responsible for ensuring compliance with virtually all of the rules and regulations* that may impact the corporation and all of its employees.

Lecture

08

Board Organization And Governance Rules

- A board is an independent high-level committee that can set many of its own rules.
- While many if not most boards and their members exercise prudent care over the corporations they govern, there will always be boards of directors that make high-risk, bad, or even criminal decisions.
- When this occurs, they can be subject to criticism or even legal action by stockholders or actions by regulatory authorities

Lecture
08

Board Organization And Governance Rules

- While ERM and a strong overall set of GRC principles **will not prevent** a board from making high-risk or bad decisions, they can **provide some help and guidance** for making better decisions on a board or board committee level.
- Because a board of directors is structured on a different level than a typical hierarchical business enterprise, we often forget that a board operates in a majority-rule committee structure.

Corporate Charters and The Board Committee Structure

Lecture

08

Importance of GRC
Principles in the Board
Room

PMG 611
Enterprise Risk Management

Lecture

08

Corporate Charters and The Board Committee Structure

- A corporate charter is the authorizing document setting the high-level rules and procedures for a corporation.
- These documents establish the basic governance rules for a corporation, such as the size and terms of service of board members and board meeting voting arrangements.
- Similar to a constitution for a country or political unit.

Lecture

08

Corporate Charters and The Board Committee Structure

- Most board meeting activities are relatively confidential.
- Much of a board's activities take place through a series of specialized committees, such as:
 - Audit Committee
 - Nominating Committee
 - Compensation Committee

Lecture

08

Corporate Charters and The Board Committee Structure

- **Audit Committee:** responsible for supervising the internal audit function, hiring and managing external auditors, approving periodic financial reports, and many other primarily financial-related activities
- **Nominating Committee:** responsible for helping to recruit new director candidates
- **Compensation Committee:** officer- and bonus-related decisions reviews and approves stock option and other deferred benefit programs.

Establishing a Board-Level Risk Committee

Lecture

08

Importance of GRC
Principles in the Board
Room

PMG 611
Enterprise Risk Management

Lecture
08

Establishing A Board-level Risk Committee

- While boards are required to have audit, nominating, and compensation committees, other committees are established based on the overall business of the corporation and other issues.
- There is a need for high-level oversight of corporate ERM activities.

Lecture
08

Establishing A Board-level Risk Committee

- In past years, corporations involved with financial instruments trading or commodities sometimes established risk committees to monitor such matters as interest rate changes or trading gains and losses.
- Others viewed many audit processes as the assessments of risks and renamed the audit committees to something like the audit and risk committee.
- However, these revised committee structures or nonconventional names did not necessarily change practices for a board's management and assessments of risks.

Lecture

08

Establishing A Board-level Risk Committee

- With the growing attention given to many aspects of risk management at major corporations, the establishment of chief risk officers (CROs)
- Growing number of corporate boards are beginning to establish separate risk management committees.
- A **Risk Committee** is a relatively new committee concept or function for many corporate boards today.

Requirements for a Risk Committee Board Member

Lecture 08

Importance of GRC Principles in the Board Room

PMG 611
Enterprise Risk Management

Lecture

08

Requirements for a Risk Committee Board Member

- These board-level committees directly supervise the activities of the CRO, monitor risk issues at a very high level, coordinate closely with the audit committee, and communicate risk-related issues with the overall board.
- Experience from ***Audit Committee*** can provide some guidance regarding what a board should consider as it is establishing requirements for a Board ***Risk Committee***.

Lecture
08

Requirements for a Risk Committee Board Member

- A *first and very important one* is that risk committee members must be nonemployee directors.
- Just as directors on the *audit committee must be nonemployees* and independent from the financial functions that are being audited, a similar level of director independence is needed for assessments and decisions on when to properly review and accept potentially risky activities.

Lecture
08

Requirements for a Risk Committee Board Member

- Today's board risk committee of nonemployee directors should have at least one director who has some demonstrated risk management qualifications.

Qualification or Experiences to Obtain Risk Management Attributes: The risk management expert must have acquired these attributes through one or more of the following means:

- Education or experience as a principal risk management officer, key internal audit or financial executive, or in a consulting firm performing significant risk management activities.
- Experience in actively supervising one or more persons actively managing such risk management functions.
- Other relevant experience.

Lecture
08

Requirements for a Risk Committee Board Member

Attributes: The board risk management expert must have the following attributes:

- A good understanding of the COSO ERM model with an emphasis on techniques for risk identification, qualitative and quantitative risk assessment approaches, and risk monitoring.
- Experiencing in analyzing and developing appropriate response plans for a broad range of financial and operational risks in active organizational environments, or experience in actively managing one or more persons engaged in risk management activities.
- An understanding of financial and general internal controls and procedures, with an emphasis on financial reporting requirements.
- A strong understanding of general governance issues facing the enterprise as well as appropriate local, national, and international regulatory issues.
- A general understanding of information systems risks, including security and telecommunications.
- An understanding of risk committee functions and how they interrelate with those of the audit committee.

ERM and Corporate Governance

Lecture
08

Importance of GRC Principles in the Board Room

PMG 611
Enterprise Risk Management

Lecture
08

ERM and Corporate Governance

- The board of directors plays a critical role in overseeing an enterprise-wide approach to risk management.
- Because management is accountable to the board of directors, the board's focus on effective risk oversight is critical to setting the **tone and culture** toward effective risk management through **strategy setting, formulating high-level objectives**, and approving broad-based resource allocations.
- COSO ERM highlights four areas that contribute to board oversight with regard to enterprise risk management:

Lecture
08

ERM and Corporate Governance

1- Understand the Enterprise's Risk Philosophy and Its Entity's Risk Appetite.

- Risk appetite is the amount of risk, on a broad level, an organization is willing to accept in pursuit of stakeholder value.
- Because boards represent the views and desires of the enterprise's key stakeholders, management should have an active discussion with the board to establish a mutual understanding of their overall appetite for risks.

ERM and Corporate Governance

2- Know the Extent to Which Management Has Established Effective Enterprise

Risk Management Processes.

- Boards should inquire as to the extent of existing risk management processes and challenge management to demonstrate the effectiveness of those processes in identifying, assessing, and managing the enterprise's most significant enterprise-wide risk exposures.

Lecture
08

ERM and Corporate Governance

3- Review the Enterprise's Portfolio of Risk and Consider It Against Their Risk Appetite.

- Effective board oversight of risks is depending on the ability of the board to understand and assess the enterprise's strategies with risk exposures.
- Board assessments should integrate strategy and operational initiatives with enterprise-wide risk exposures, and this should strengthen the ability of a board to ensure that risk exposures are consistent with overall appetite for risk.

Lecture
08

ERM and Corporate Governance

4- Be Apprised of the Most Significant Risks and Whether Management Is Responding Appropriately.

- Risks are constantly evolving and the need for robust information is high.
- Regular updating by management to boards of key risk indicators is critical to effective board oversight of key risk exposures for preservation and enhancement of stakeholder value.

Summary

Lecture
08

Importance of GRC Principles in the Board Room

PMG 611
Enterprise Risk Management

Lecture
08

Summary

- A board of directors has many responsibilities in managing the overall operation of a corporation.
- Risk oversight and the management of risks are major components of those activities and board responsibilities.

“The board’s role, quite simply, is to provide risk oversight.

This means making sure that management has instituted processes to identify, and bring to the board’s attention, the major risks the enterprise faces. It also means the continual reevaluation of these monitoring processes and the risks with the help of the board and its committees.”

Lecture

08

Summary

- Board Members must try to identify the potential risks facing their enterprise and then try to understand the potential implications and consequences of these various risks.
- This can be daunting for the board member who only receives supporting data about an upcoming potential risk-based decision, has an opportunity to ask further questions about the matter and then must vote to take appropriate actions regarding that risk.

Lecture

08

Summary

- Boards of directors use their board committees in carrying out certain of their risk oversight duties.
- Some enterprises may choose to start the process by asking the relevant committees to address risk oversight in their areas while focusing on strategic risk issues in the full board discussion.
- Robust engagement by the board in enterprise risk oversight strengthens an enterprise's resilience to significant risk exposures.

References

- COSO Enterprise Risk Management: Establishing Effective Governance, Risk, and Compliance Processes. Robert R. Moeller.



Thank You