

Enterprise Risk Management

PMG 611

Lecture 3

Importance of Effective GRC Practices
and Principles

Prepared by
Dr. Eng. Abdullah Jameel Halawany

Lecture

0

Session Outline

Introduction

Road to
Effective GRC
Principles

Importance of
GRC
Governance

Risk
Management
Component of
GRC

GRC and
Enterprise
Compliance

Importance of
Effective GRC
Practices and
Principles

Introduction

Lecture

03

Importance of Effective GRC Practices and Principles

PMG 611

Enterprise Risk Management

Lecture

03

Introduction

- Enterprise organizations and corporations have faced governance issues since their earliest days.
- In past eras, setting the rules for employees and other stakeholders to follow worked with small single proprietorships or in the tightly centralized corporations.
- Today's larger and often multiunit enterprises need broad-based units or functions for setting rules and procedures—they need efficient and effective governance processes.

Lecture

03

Introduction

- Life would be easier for enterprises if they just had to rely on a central leadership to set those governance rules.
- Enterprises today of any location or size are faced with ever **increasing** sets of **rules** and **procedures**
 - Local Police
 - Public Safety Ordinances
 - National and International Laws
 - Broad professional rules and standards

Lecture

03

Introduction

- On a whole series of levels, an enterprise must comply with these laws and regulations.
- Failure to do so can result in a variety of *penalties*.
- Enterprise *needs processes* to ensure that they are operating in compliance with the appropriate laws and regulations.
- An enterprise always faces *risks* that it will be found in **violation** of one or another of these multiple laws and regulations.

Lecture

03

Introduction

- There are also risks that their own established governance rules will
 - not achieve their desired results or
 - may face some outside event beyond their control, such as a major weather event or a fire
- There is a need to *manage* these risks at an *overall enterprise level*.
- **ERM** has brought all three of these *Governance*, *Risk*, and *Compliance* concerns together into what has been called **GRC** principles.

Road to Effective GRC Principles



Lecture

03

Importance of Effective GRC Practices and Principles

PMG 611

Enterprise Risk Management

Lecture
03

Road to Effective GRC Principles

- Business professionals did not even hear about the now increasingly familiar acronym GRC until a few years after SOx.
- The Sarbanes-Oxley Act of 2002, often simply called SOX or Sarbox, is U.S. law meant to protect investors from fraudulent accounting activities by corporations.
- Sarbanes-Oxley was enacted after several major accounting scandals in the early 2000's perpetrated by companies such as Enron, Tyco, and WorldCom.

Lecture
03

What is SOX Law?

- The law mandates strict reforms to improve financial disclosures from corporations and prevent accounting fraud.
- It also covers issues such as auditor independence, corporate governance, internal control assessment, and enhanced financial disclosure.
- The law is named for the two congressmen who drafted it, Paul Sarbanes and Michael Oxley.
- The U.S. Securities and Exchange Commission (SEC) administers the act.

Lecture

03

G for Governance

- It means taking care of business, making sure that things are done according to
 - Enterprise's Standards,
 - Enterprise's Regulations,
 - Enterprise's Board of Directors' Decisions.
- It also means setting forth clear stakeholder expectations of what should be done so that everyone is on the same page with regard to how the enterprise is run.

Lecture

03

R for Risk

- It's pretty clear that certain risks are just not to be taken.
- When it comes to business, however, risk becomes a way to help both
 - Protect existing asset value
 - Create value by strategically expanding an enterprise or adding new products and services.
- The concept of risk is even more important than just the ERM. (Lecture 2)

Lecture
03

C for Compliance

- Represents compliance with the many laws and rules affecting businesses and citizens today.
- Sometimes, people will also extend that C to include controls.
- For example, it means monitoring a factory's emissions or ensuring that its import and export papers are in order. Or it might just mean establishing effective *Internal Accounting Controls*.

Lecture

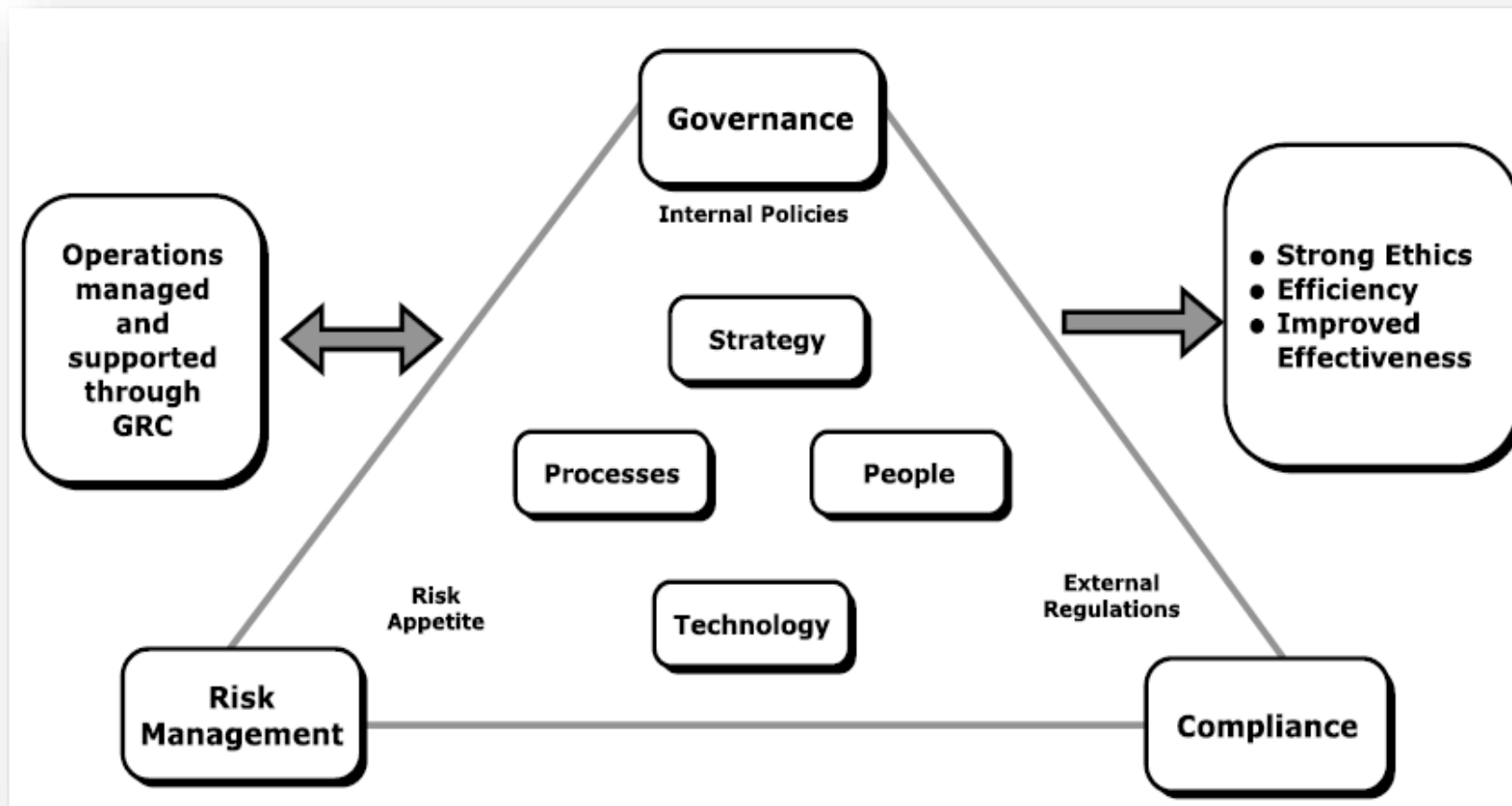
03

GRC Concepts

- All enterprises, and corporations, historically do not think of GRC as a combined set of principles.
- **GRC** is an increasingly recognized term that reflects a new way in which enterprises today are adopting an integrated approach to these aspects of their businesses.
- **GRC** represent core disciplines of governance, risk management, and compliance.
- Each of the disciplines consists of the four basic GRC components: **strategy**, **processes**, **technology**, and **people**.

Lecture
03

GRC Concepts



Lecture

03

GRC Concepts

- Internal policies are the key factors supporting governance.
- External regulations drive compliance principles.
- Enterprise's risk appetite is a key element of risk management.
- Requires *management attention* and *support*,
- Result in ***correct ethical behavior***, organizational ***efficiency***, and ***improved effectiveness***

GRC Concepts

- The three GRC principles should be thought of in terms of one continuous and interconnecting flow of concepts.
- **Neither** G, R, or C more important or significant than the others.

Importance of GRC Governance

Lecture

03

Importance of Effective GRC Practices and Principles

PMG 611

Enterprise Risk Management

Lecture
03

Importance of GRC Governance

- Corporate or enterprise governance is a term that refers broadly to the rules, processes, or laws by which businesses are operated, regulated, and controlled.
- The term can refer to
 - Internal factors defined by the officers, stockholders, or the charter and basic objectives of a corporation.
 - External forces such as consumer groups, clients, and government regulations.

Lecture

03

Importance of GRC Governance

- At enterprise operations level, we can define enterprise governance as
- The responsibilities and practices *exercised* by the board, executive management, and all levels of functional management *with the goals* of
 - Providing strategic direction.
 - Ensuring that objectives are achieved.
 - Ascertaining that risks are managed appropriately.
 - Verifying that the enterprise's resources are used responsibly.

Lecture
03

Importance of GRC Governance

- Governance really refers to the process of
 - **Establishing** rules and procedures within all levels of an enterprise
 - **Communicating** those rules to appropriate levels of stakeholders
 - **Monitoring** performance against those rules
 - **Administering** rewards and punishments based on the relative performance or compliance with those rules

Lecture
03

Importance of GRC Governance

- A well-defined and enforced set of corporate governance principles provides a *structure* that works for the benefit of everyone concerned by ensuring that the enterprise adheres *to accepted ethical standards* and *best practices* as well as to *formal laws*.

GRC Governance Concepts



Risk Management Component of GRC

Lecture

03

Importance of Effective GRC Practices and Principles

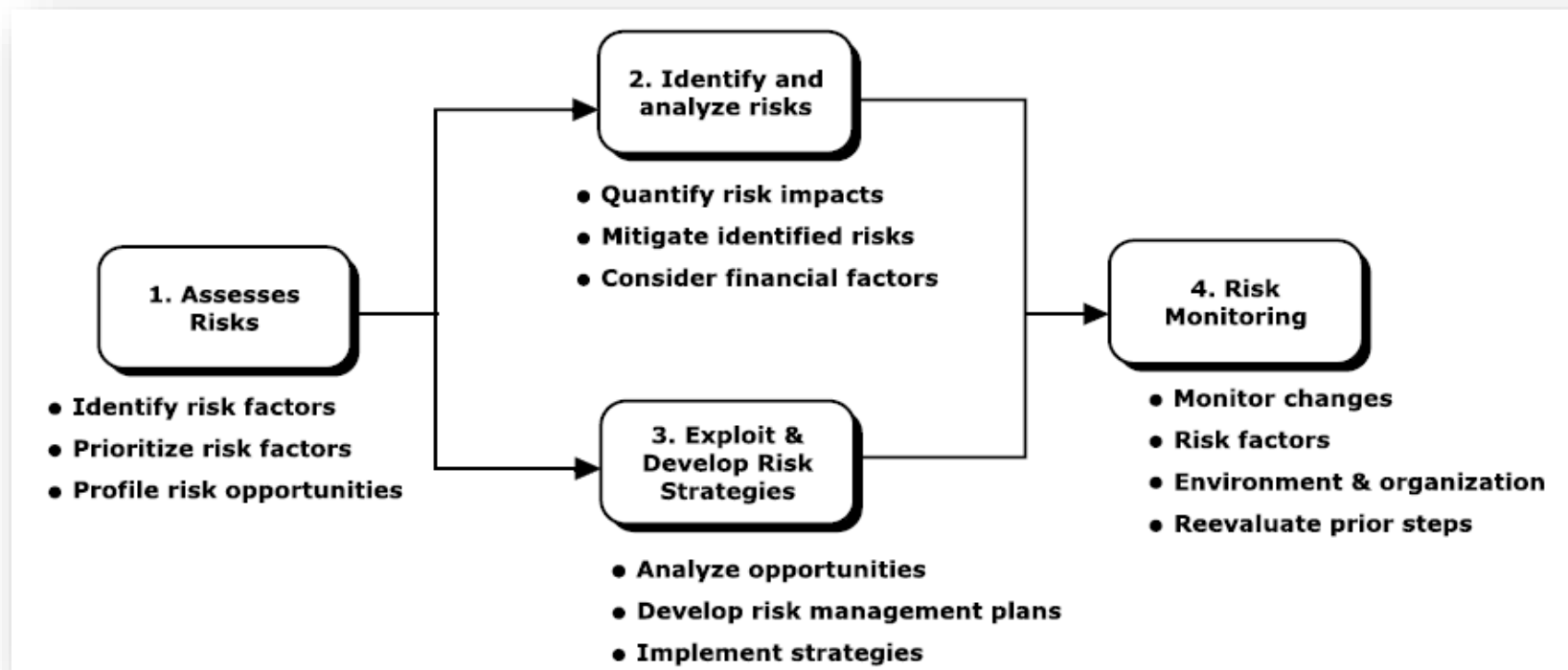
PMG 611

Enterprise Risk Management

Lecture
03

Risk Management Component of GRC

- **Risk Management** should be part of the overall enterprise culture from the board of directors and very senior officers down through the enterprise.



Lecture
03

Risk Management Component of GRC

1- Risk assessment and planning.

- Any enterprise faces all levels of risks, whether global issues based on weather or currency threats to weather-related threats at local operations.
- We cannot plan or identify every type of risk that might impact an enterprise, but there should be an ongoing analysis of these various potential risks that may face an enterprise.

Lecture
03

Risk Management Component of GRC

2- Risk identification and analysis

- There is a need for a more detailed analysis on the likelihood of these risks coming to fruition as well as their potential impacts.
- There is a need to quantify the impacts of the identified risks and to determine mitigation strategies in the event the risk event occurs.
- Mitigation refers to assessing the best way to manage or eliminate an identified risk.

Lecture
03

Risk Management Component of GRC

3- Exploit and develop risk response strategies.

- Essentially a concept that should be considered in parallel with risk identification, an enterprise should develop plans and strategies to return to normal operations and then recover from the risk event.
- This may include an analysis of risk-related opportunities.

Lecture
03

Risk Management Component of GRC

4- Risk monitoring.

- Tools and facilities should be in place to monitor for the identified risks possibly occurring.
- Most risk-related monitoring requires a wide series of special reports, established and measurable standards, and a diligent human resources function.
- The idea is to keep ahead and to reenter these prior risk management steps as necessary.

GRC and Enterprise Compliance



Lecture

03

Importance of Effective GRC Practices and Principles

PMG 611

Enterprise Risk Management

Lecture
03

GRC and Enterprise Compliance

- Compliance is the process of adhering to a set of guidelines or rules established by government agencies, standards groups, or internal corporate policies.
- These is applied to all types of business.
- Adhering to these compliance-related requirements is a challenge

Lecture
03

GRC and Enterprise Compliance

- Adhering to these compliance-related requirements is a challenge because of
 - The frequent introduction of new regulations.
 - Vaguely written regulations that require interpretation.
 - No consensus on best practices used for compliance.
 - Multiple regulations often overlap.
 - Constantly changing regulations.

Lecture
03

GRC and Enterprise Compliance

The Frequent Introduction Of New Regulations

- Regulation is a fundamental tool for managing the risks present in society and the economy and can help to reduce the incidence of hazardous events and their severity.
 - Examples (New studies, Privacy issues, etc..)
- Companies have a challenge to monitor these rules and determine which apply to them.

Lecture
03

GRC and Enterprise Compliance

Vaguely Written Regulations That Require Interpretation

- Some regulations was printed on many thousands of pages, covering issues and rules that the legislators who passed the bill never even read, let alone understood.
- Even today, we are still looking at these rules and interpreting what they mean.
- Compliance with those types of rules can be difficult.

Lecture
03

GRC and Enterprise Compliance

No Consensus On Best Practices Used For Compliance

- **Diverse Regulations:** Different industries and regions have varying compliance requirements. This diversity makes it challenging to establish a universal set of best practices.
- **Evolving Standards:** can lead to differing opinions on what constitutes best practices.
- **Varied Organizational Needs:** What works for one company may not be applicable for another, leading to a lack of consensus.
- **Stakeholder Perspectives:** Different stakeholders may prioritize different aspects of compliance, such as cost-effectiveness, risk management, or ethical considerations.

Lecture
03

GRC and Enterprise Compliance

Multiple Regulations Often Overlap

- Governmental units from different geographies may issue rules that cover similar areas but may have different requirements.
- Compliance until matters are resolved can be a challenge.

Lecture
03

GRC and Enterprise Compliance

Constantly Changing Regulations

- Regulatory agencies in particular are often constantly changing or reinterpreting their rules, making strict compliance a challenge.
- Examples (Ex post evaluation of past approaches)

Lecture

03

GRC and Enterprise Compliance

- Compliance becomes a continuous process, not a one-time project.
- Continues to drive business agendas as organizations are being held accountable for meeting the myriad of mandates specific to their markets.
- Enterprises might also be required to address cross-industry legislation.

Scope of Compliance Architectures Considerations

- The scope of compliance also permeates other aspects of an enterprise.

Scope of Compliance	Area for Considerations
Strategy	■ As an organization develops its strategy, it must determine which regulations are relevant. ■ Compliance sustainability needs to be an integral part of any compliance strategy.
Organization	■ The organizational structure must be established to meet the specific requirements (or intent) of each regulation (e.g., Sarbanes-Oxley recommends the Chief Executive Officer and President be two different people).
Processes	■ Key processes must be documented and practiced. ■ Audits or reviews must take place to ensure documented processes are effectively being used to address compliance/regulation requirements.
Applications and data	■ Applications must be designed, implemented and continuously tested to support the requirements of each regulation. ■ Data must be properly protected and handled according to each regulation.
Facilities	■ Facilities must be designed and available to meet the needs of each regulation (i.e., some regulations may require records to be readily available at an off-site location).

Importance of Effective GRC Practices and Principles

Lecture

03

Importance of Effective GRC Practices and Principles

PMG 611

Enterprise Risk Management

Lecture

03

Importance of Effective GRC Practices and Principles

- Corporate Governance has received increased attention because of high-profile scandals involving abuse of corporate power and, in some cases, alleged criminal activity by corporate officers.
- An integral part of an effective corporate governance regime includes provisions for civil or criminal prosecution of individuals who conduct unethical or illegal acts in the name of the enterprise.

Lecture

03

Importance of Effective GRC Practices and Principles

- Risk management should create value and be an integral part of organizational processes.
- It should be part of decision-making processes and be tailored in a systematic and structured manner to explicitly address the uncertainties an enterprise faces based on the best available information.
- In addition, risk management processes should be dynamic, iterative, and responsive to change with the capabilities of continual improvements and enhancements.

Lecture

03

Importance of Effective GRC Practices and Principles

- A consistent approach on the use of compliance driven capabilities and supporting technologies across an enterprise can provide these potential benefits:
 - Reduced total cost of ownership.
 - Flexibility.
 - Competitive advantage.

Lecture

03

Importance of Effective GRC Practices and Principles

- **Reduced total cost of ownership.**
 - For example, many regulations specify document retention requirements, which can be met by a single investment in a content and records management system.
- **Flexibility.**
 - By centrally managing compliance initiatives via organization-wide compliance architecture, an enterprise can quickly adapt to these changes.
- **Competitive advantage.**
 - Better understand and control their business processes, which allows them to respond more quickly and accurately to external or internal pressures.

Summary

Lecture

03

Importance of Effective GRC Practices and Principles

PMG 611

Enterprise Risk Management



GRC Governance Concepts



3-23

Scope of Compliance Architectures Considerations

- The scope of compliance also permeates other aspects of an enterprise.

Scope of Compliance	Area for Considerations
Strategy	- As an organization develops its strategy, it must determine which regulations are relevant. - Compliance sustainability needs to be an integral part of any compliance strategy.
Organization	The organizational structure must be established to meet the specific requirements (or intent) of each regulation (e.g., Sarbanes-Oxley recommends the Chief Executive Officer and President be two different people).
Processes	- Key processes must be documented and practiced. - Audits or reviews must take place to ensure documented processes are effectively being used to address compliance/regulation requirements.
Applications and data	- Applications must be designed, implemented and continuously tested to support the requirements of each regulation. - Data must be properly protected and handled according to each regulation.
Facilities	Facilities must be designed and available to meet the needs of each regulation (i.e., some regulations may require records to be readily available at an off-site location).

3-39

Lecture

03

Risk Management Component of GRC

- Risk Management** should be part of the overall enterprise culture from the board of directors and very senior officers down through the enterprise.



3-25

3-47

References

- COSO Enterprise Risk Management: Establishing Effective Governance, Risk, and Compliance Processes. *Robert R. Moeller.*
- Implementing Enterprise Risk Management: From Methods To Applications. *James Lam.*



Thank You