

PMG 611

Enterprise Risk Management

Prepared by:
Dr. Abdullah Jameel Halawany

Lecture 1



Lecture 1

Dr. Eng. Abdullah Jameel Halawany

ahalawany@esu.edu.sa

- PhD in Industrial Engineering
 - University of Central Florida, Orlando, FL, USA
- Project Engineering Certificate
- Quality Assurance Certificate
- Six Sigma Green Belt Certificate
- Trainer of Trainee (TOT)
- Professional Engineer Certificate



Lecture 1

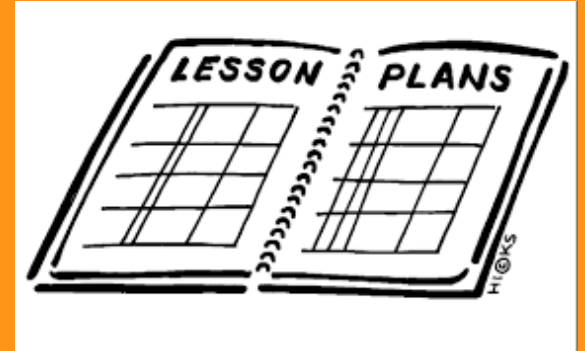
Session Outline

Introduction to the Course

- Learning Platform
- References
- Brief Description
- Topics
- Learning Outcomes

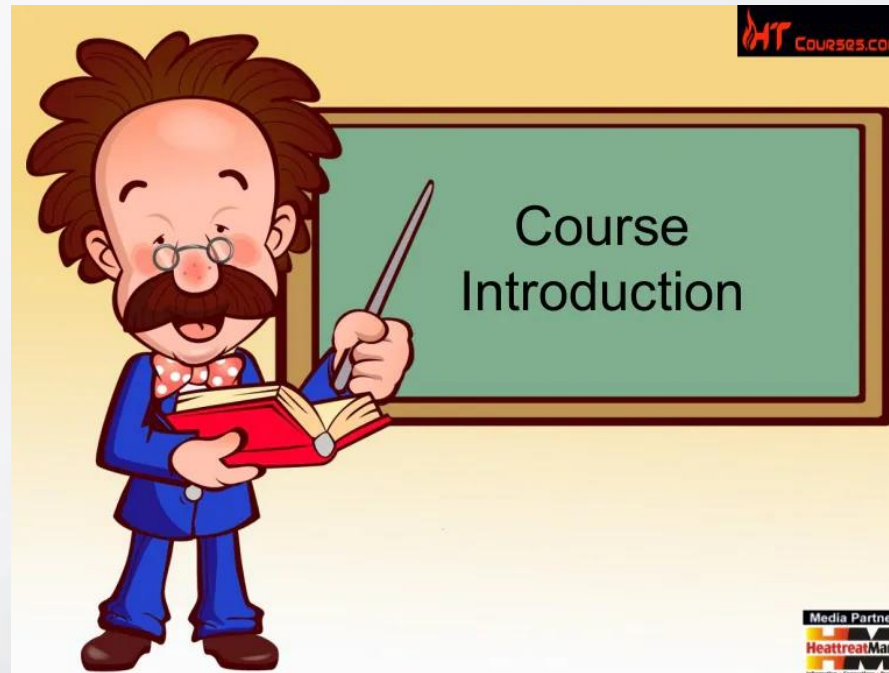
ERM

- ERM History and Drivers
- What is ERM?
- Benefits of ERM
- Clearing Misconceptions
- Internal Control vs. ERM
- ERM Limitations
- Summary



Lecture 01

Introduction to the course



Lecture 1

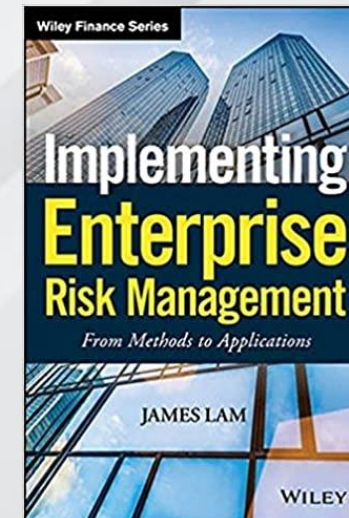
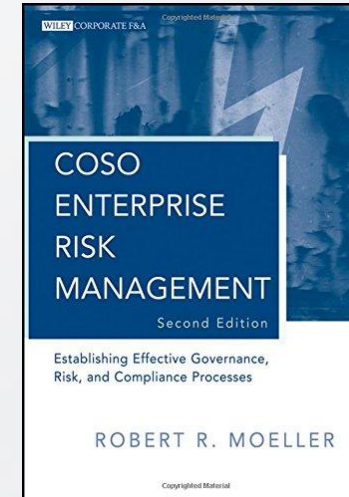
Learning Platform

- <https://lms.midocean.ae/>
- IT MUST be checked frequently
- Include All course material and information
 - Lectures' Videos and PDF/PPT files
 - Course grades distribution
 - Quizzes/Assignments/Exams Dates
 - Regulations for accepted excuses
 - Zoom weekly meeting link (same link is used for all meetings)

Lecture 1

References

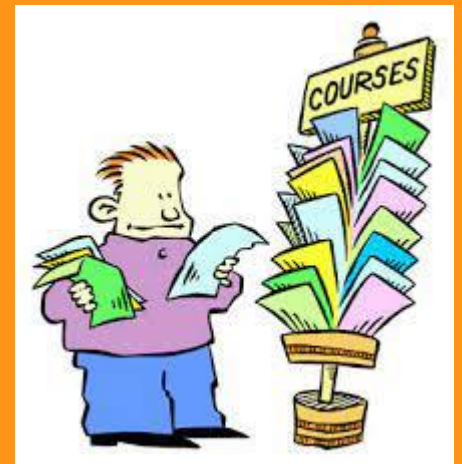
- COSO Enterprise Risk Management: Establishing Effective Governance, Risk, and Compliance Processes. Robert R. Moeller.
- Implementing Enterprise Risk Management: From Methods To Applications. James Lam.



Lecture 1

Brief Description of The Course

- In Enterprise Risk Management, we develop a holistic approach to the identification and management of risks facing an organization, allowing leaders to identify and quantify the risks facing the enterprise.
- This course will present management tools and frameworks to understand and identify risk.
- Emphasis will be placed on how to improve a firm's risk position, and how to adapt an organization to deal with risk.
- In addition, this course discusses issues related to the implementation of risk management systems and compliance with key regulatory requirements, and the importance of Governance, Risk, and Compliance Principles (GRC).



Lecture 1

Topics

Introduction to Enterprise Risk Management

Risk Management Fundamentals and Risk Portfolio Management

Importance of Governance, Risk, and Compliance Principles and Practices.

ERM Frameworks: COSO ERM Frameworks, ISO 31000, and 38500 Risk Management Worldwide Standards

Implementing ERM in the Enterprise

Integration of KPIs and KRIs and ERM Dashboard Reporting

Enterprise Compliance Issues Today

Role of Internal Audit in Enterprise Risk Management

Importance of GRC Principles in the Board Room

Cybersecurity and Information Technology and Enterprise Risk Management

Establishing an Effective GRC Culture throughout the Enterprise

ERM and GRC Principles Going Forward



Lecture 1

Course Learning Outcomes

- 1- Provide a definition of risk and describe why risk management is important.
- 2- Understand the Importance of Governance, Risk, and Compliance Principles
- 3- Describe the elements of an ERM framework.
- 4- Identify the obstacles to effective risk management.
- 5- Recognize and be able to discuss the rising expectations for risk management to be more strategic and value-adding.
- 6- Identify some of the organizational arrangements, processes and culture that enable successful risk management.
- 7- Clarify what KRIs are and demonstrate their practical applications and value to an organization.

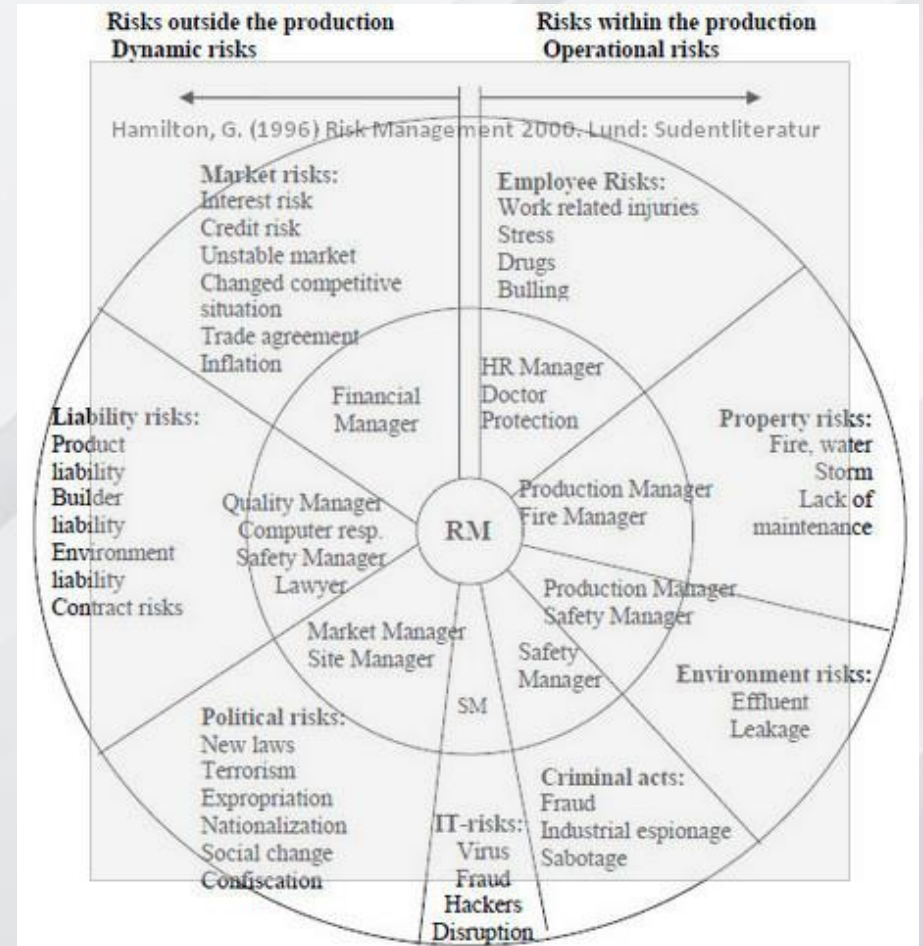


Enterprise Risk Management (ERM) History and Drivers

- Protecting ourselves against risk is a natural practice.
- In fact, one could argue that risk management has existed as long as human history.
- Despite the intuitive nature of risk management—or perhaps because of it—it did not become part of formal business practice until the second half of the last century.
- It wasn't until 1963 that the first discussion on risk appeared in an attempt to codify and improve such practices.

Enterprise Risk Management (ERM)

- The concept of a holistic approach of ERM traces its roots to the early 1970s when Gustav Hamilton proposed the “Risk Management Circle” to describe the interaction of all elements in the risk management process (assessment, control, financing and communication).



Enterprise Risk Management (ERM)

- In the 20th century, risk managers were primarily responsible for managing "pure" risks through the purchase of insurance.
- The concept of risk management soon became associated with financial risk management with the use of derivative financial products.
- There are several checkpoints that have driven the need for enterprise risk management.

- This includes an increase in:
 - Greater transparency
 - Financial disclosures with more strict reporting and control requirements
 - Security and technology issues
 - Business continuity and disaster
 - Focus from rating agencies
 - Regulatory compliance
 - Globalization in a continuously competitive environment

What is ERM?

- Events can have **negative impact**, **positive impact**, or both.
- Events with a negative impact represent **risks**, which can prevent value creation or erode existing value.
- Events with positive impact may offset negative impacts or represent opportunities.
- Opportunities are the possibility that an event will occur and positively affect the achievement of objectives, supporting value creation or preservation.
- Management channels opportunities back to its strategy or objective-setting processes, formulating plans to seize the opportunities.

What is ERM?

- All organizations need to set strategy and periodically adjust it, always staying aware of
 - ever-changing opportunities for creating value
 - the challenges that will occur in pursuit of that value.
- To do that, they need the best possible framework for optimizing strategy and performance.

What is ERM?

*“is a **methodology** that looks at risk management **strategically** from the perspective of the **entire** firm or organization. It is a top-down strategy that aims to identify, assess, and prepare for potential losses, dangers, hazards, and other potentials for harm that may **interfere** with an organization's operations and objectives and/or lead to losses.”*

What is ERM?

Definition by Committee of Sponsoring Organizations of the Treadway Commission (COSO)

“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**.”

Lecture 01

WHAT IS ERM?

It is the capability to effectively answer the following questions:



- Circular depiction is highly intentional
- Components are meant to be dynamic (reviewed back/forth in any sequence)
- Having the right culture is key

Benefits of ERM

Benefits of ERM

- Organizations that integrate enterprise risk management throughout the entity can realize many benefits, including, though not limited to:
 - Increasing the range of opportunities
 - Identifying and managing risk entity-wide
 - Increasing positive outcomes and advantage while reducing negative surprises
 - Reducing performance variability
 - Improving resource deployment
 - Enhancing enterprise resilience

- **Increasing the range of opportunities**

- By considering all possibilities—both positive and negative aspects of risk—management can identify new opportunities and unique challenges associated with current opportunities.

- **Identifying and managing risk entity-wide**

- Countless risks that can affect many parts of the organization. Sometimes a risk can originate in one part of the entity but impact a different part. Consequently, management identifies and manages these entity-wide risks to sustain and improve performance.

- **Increasing positive outcomes and advantage while reducing negative surprises**
 - ERM improve ability to identify risks and establish appropriate responses, reducing surprises and related costs or losses, while profiting from advantageous developments.
- **Reducing performance variability**
 - Performing ahead of schedule or beyond expectations may cause as much concern as performing short of scheduling and expectations.
 - ERM allows organizations to anticipate the risks that would affect performance and enable them to put in place the actions needed to minimize disruption and maximize opportunity.

Benefits of ERM

- **Improving resource deployment**

- Every risk could be considered a request for resources. Obtaining robust information on risk allows management, in the face of finite resources, to assess overall resource needs, prioritize resource deployment and enhance resource allocation.

- **Enhancing enterprise resilience**

- An entity's medium- and long-term viability depends on its ability to anticipate and respond to change, not only to survive but also to evolve and thrive. It becomes increasingly important as the pace of change accelerates and business complexity increases.

Clearing Up a Few Misconceptions

Clearing Up a Few Misconceptions

“Enterprise risk management is not a function or department.”

- It is the culture, capabilities, and practices that organizations integrate with strategy-setting and apply when they carry out that strategy, with a purpose of managing risk in creating, preserving, and realizing value.

Clearing Up a Few Misconceptions

“Enterprise risk management is more than a risk listing.”

- It requires more than taking an inventory of all the risks within the organization.
- It is broader and includes practices that management puts in place to actively manage risk.

Clearing Up a Few Misconceptions

“Enterprise risk management is not a checklist.”

- It is a set of principles on which processes can be built or integrated for a particular organization, and it is a system of monitoring, learning, and improving performance.

Clearing Up a Few Misconceptions

“Enterprise risk management can be used by organizations of any size.”

- If an organization has a mission, a strategy, and objectives—and the need to make decisions that fully consider risk—then enterprise risk management can be applied.
- It can and should be used by all kinds of organizations, from small businesses to community-based social enterprises to government agencies to Fortune 500 companies.

Clearing Up a Few Misconceptions

“Enterprise risk management addresses more than Internal Control.”

- It also addresses other topics such as strategy-setting, governance, communicating with stakeholders, and measuring performance.
- Its principles apply at all levels of the organization and across all functions.

Internal Control vs. ERM

Internal Control

- **Internal control** is a process, effected by an entity's board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives relating to **operations**, **reporting**, and **compliance**.

Operations – Effectiveness and efficiency of operations

Reporting – Reliability of reporting for internal and external use

Compliance – Compliance with applicable laws and regulations”

Internal Control

- **Internal control** is indeed important to developing reasonable assurance that the applicable processes will operate as designed and achieve the desired objectives.
- Organizations can have **objectives outside** of these three categories.
- Any choice of a future action typically entails risk.
- Those choices extend far beyond the execution of currently implemented business processes and include any decision for future action not dependent on an existing process.

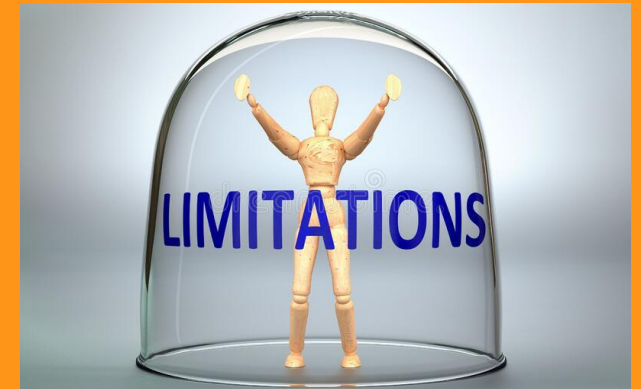
ERM Encompasses Internal Control

- **Internal control** is an integral part of enterprise risk management.
- This enterprise risk management framework encompasses internal control, forming a more robust conceptualization and tool for management

Lecture 1

ERM Limitations

- **Human judgment** in decision making can be faulty
- Decisions on responding to risk and establishing controls need to consider the relative *costs* and *benefits*, breakdowns can occur because of human failures such as simple errors or mistakes
- Controls can be circumvented by collusion of two or more people
- Management has the ability to override enterprise risk management decisions.
- These limitations prevent a board and management from having absolute assurance as to achievement of the entity's objectives.

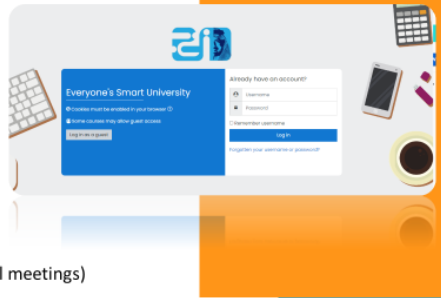


Summary

Lecture 01

Lecture 1 Learning Platform

- <https://moodle.esu.edu.sa/>
- IT MUST be checked frequently
- Include All course material and information
 - Lectures' Videos and PDF/PPT files
 - Course grades distribution
 - Quizzes/Assignments/Exams Dates
 - Regulations for accepted excuses
 - Zoom weekly meeting link (same link is used for all meetings)



Lecture 01 Event

- Events can have **negative impact**, **positive impact**, or both.
- Events with a negative impact represent **risks**, which can prevent value creation or erode existing value.
- Events with positive impact may offset negative impacts or represent opportunities.
- Opportunities are the possibility that an event will occur and positively affect the achievement of objectives, supporting value creation or preservation.
- Management channels opportunities back to its strategy or objective-setting processes, formulating plans to seize the opportunities.



L1 - 16

Lecture 01 What is ERM?

Definition by Committee of Sponsoring Organizations of the Treadway Commission (COSO)"

"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**."



L1 - 19

L1 - 38

Lecture 01

- **ERM**: Enterprise Risk Management
- **GRC**: Governance, Risk, and Compliance
- **RM**: Risk Management
- **COSO**: Committee of Sponsoring Organizations of the Treadway Commission

WHAT IS ERM? It is the capability to effectively answer the following questions:



- Circular depiction is highly intentional

- Components are meant to be dynamic (reviewed back/forth in any sequence)

- Having the right culture is key

References

COSO Enterprise Risk Management: Establishing Effective Governance, Risk, and Compliance Processes

Guidance on Enterprise Risk Management.

<https://www.coso.org/Pages/erm.aspx>