

Enterprise Risk Management

PMG 611

Lecture 5

Implementing ERM in the Enterprise

Prepared by
Dr. Eng. Abdullah Jameel Halawany

Lecture
05

Session Outline

Roles and
Responsibilities
of an Enterprise
Risk
Management
Function

ERM Activity
Scope and
Review Planning

Risk
Management
Policies,
Standards, and
Strategies

Risk
Management
Reviews and
Corrective
Action Practices

Introduction

Lecture

05

Implementing ERM in the Enterprise

PMG 611
Enterprise Risk Management

Lecture

05

Introduction

- Virtually, all larger public companies today have some type of ***Risk Management Department*** or function.
- Their formal enterprise risk management was structure as a lower-level department which often was primarily responsible for purchasing insurance and implementing routine loss prevention programs for certain high-frequency exposures.
- That risk management function usually did not receive the respect it should deserve in today's era of ERM.

Lecture

05

Introduction

- Those *Risk Management Functions* were not structured at a senior or C-level status in enterprise charts.
- An effective *Risk Management Function* would be headed by a *Chief Risk Officer (CRO)*
- An executive whose responsibility is to ascertain that *enterprise risks* are properly *understood* and *translated* into meaningful
 - *business requirements*
 - *Objectives*
 - *metrics.*

- Even if an enterprise has a traditional “insurance department,” the ERM framework provides an enterprise with an excellent opportunity to reengineer their existing insurance-based risk management function along the lines of the ERM framework or to create a separate new ERM function for the enterprise.

Lecture

05

Introduction

- Given the importance of risk management in today's enterprise, ERM functions should *operate at a higher level* than the traditional insurance-based risk function groups that sometimes operated side by side with such facility support functions as property security and loss prevention.
- ***While these latter functions are important to an enterprise, the ERM department should take a higher and more prominent role.***

Roles and Responsibilities of an Enterprise Risk Management Function

Lecture

05

Implementing ERM in the Enterprise

PMG 611
Enterprise Risk Management

Lecture

05

Roles and Responsibilities of an
Enterprise Risk Management Function

- The responsibilities of today's enterprise risk function have been broadened and deepened to include *regulations*, *capital markets concerns*, *financial reporting*, the many issues *surrounding globalization*, *intellectual capital*, and, of course, all aspects of *IT*.
- To be effective, the enterprise risk function and its *CRO* must have their **eyes wide open** regarding the *various levels of risks* impacting all levels of the enterprise.

Lecture

05

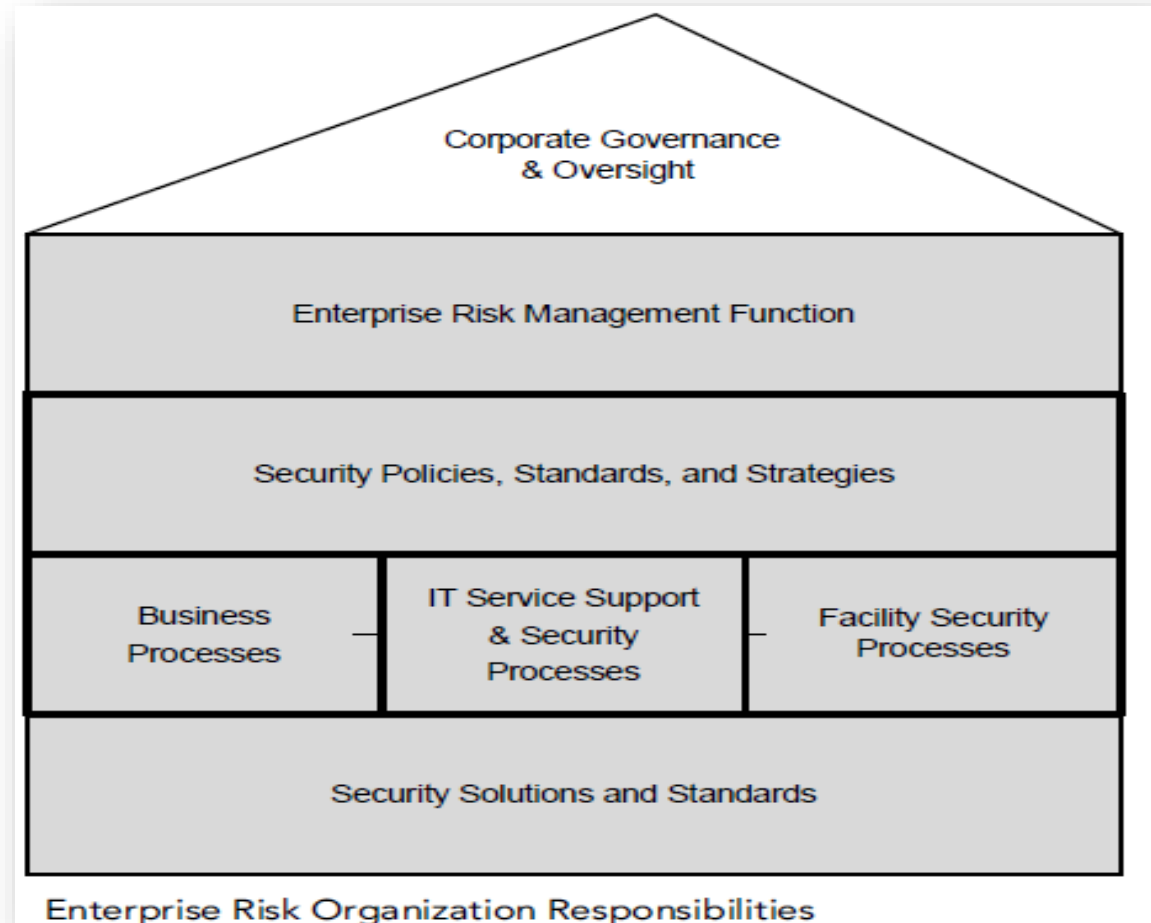
Roles and Responsibilities of an
Enterprise Risk Management Function

- For a public corporation, an enterprise risk management function should be a senior-level operating unit with authority covering the entire enterprise.
- For a larger enterprise with **multiple** and differing business operations, there may be a need for separate multiple risk management units, but all should report to a single responsible risk function headed by a **CRO**

Lecture
05

Roles and Responsibilities of an Enterprise Risk Management Function

- Whether a relatively small organization or a multidivisional, multicounty type of enterprise, any risk management function should follow these same general operational standards and guidelines.



Lecture

05

CRO Responsibilities

- A key component of an effective ERM function is the need for enterprise *leadership* that is responsible for the overall risk management process.
- *That title of “chief” means little unless the CRO has the authority and responsibility to effectively manage the enterprise risk program and to communicate these activities to senior management.*

Lecture

05

CRO Responsibilities

- The major responsibility of the CRO is
 - To manage the process of assessing risks throughout the enterprise,
 - To implement appropriate corrective actions,
 - To communicate risk issues and events to all levels of the enterprise.
 - Supporting risk management function.

Lecture
05

CRO Responsibilities

- ***Risk Management Function*** should have several staff specialists to help review and help minimize enterprise risks in addition to developing risk management policies, standards, and strategies.
- These are persons with the abilities to understand and help implement corrective actions for general business, IT, and basic insurance-related risks.
- ERM specialists should have the authority and responsibility to both identify specific enterprise risks and to actually help implement corrective actions to minimize those identified risks.

Lecture

05

Enterprise Risk Management Function vs. Internal Audit

- Internal auditors review internal controls and make recommendations for improvement
- Usually take no active role in helping to implement those recommended changes, unless specifically engaged as internal consultants.
- Very important difference between an enterprise risk management function and internal audit is that the ERM group will usually go beyond just reviewing an area and making recommendations for subsequent follow-up.

Lecture
05

Examples of How an Effective Enterprise Risk Management Function Might Operate

Take
Actions

- An enterprise *Risk Management Analyst* reviews the potential new product liability risks in a given business area.
- *Risk Management Function* may identify governmental actions that may place some foreign country operations at risk.
- An *Enterprise Risk Management Specialist* with strong IT skills may access system vulnerabilities in what is often called a firewall perimeter surrounding an area of IT operations.

ERM Activity Scope and Review Planning

Lecture

05

Implementing ERM in the Enterprise

PMG 611
Enterprise Risk Management

Lecture

05

ERM Activity Scope and Review Planning

- An effective **ERM** function should not, however, just go from one risk-related area to another without any type of organized plan or approach.
- **ERM** function should follow a **risk review plan** covering an **extended time period**.
- By its very nature, risk management will always be responding to crises as they occur, but that response should try to follow a **standard, consistent** approach **throughout the enterprise**.

Lecture

05

ERM Activity Scope

- ERM function should first *develop* an *understanding* of and *document* the risk areas that are in their scope of operations.
- There are always some risk events either too big or too little to be included within the scope of the ERM group.
- We are referring to very major events such as violent weather, major economic disruptions, and the like.

Lecture

05

ERM Activity Scope

- The CEO along with the risk management organization may be able to have some high-level risk response plans in place for such events, but often cannot realistically do much beyond having some very general plans or statements of support in place.
- Similarly, there will always be some risk areas that are perhaps troublesome difficulties but are not within the scope of the ERM group.
- Should have some internal guidelines covering the types of risks it can realistically manage.

Lecture
05

Risk Activity Scope: Example



Risk Activity Scope

Global Computer Products

The corporate Enterprise Risk Management (ERM) group is responsible for monitoring and developing remediation plans for all major corporate operational risks. Operational risks include, but are not limited to, all major activities involving the development of new company products, acquisition and maintenance of assets, legal and regulatory issues, financial reporting, and internal controls. The ERM group will establish guidelines for all risk management processes, will assign the management of some risks to appropriate operating units, but will assume the direct management of others.

ERM recognizes there are some market, economic, or environmental risks that are beyond its scope and ability to take corrective actions. ERM will communicate these risk issues with the board of directors' risk committee and will assist in risk remediation where appropriate.

Lecture

05

ERM Activity Scope

- This type of risk responsibility scope document should be an internal ERM policy statement and would not be developed for general distribution to enterprise stakeholders at large.
- It shows ERM's areas of risk management expertise, where the enterprise is responsible for various risks, and the acceptance of other entities, such as the legal department or local fire departments, for handling other risks.

Lecture

05

ERM Activity Scope

- This is the type of document that the CRO should share in a board or CEO-level briefing so that they are aware of the ERM's planned area of scope.
- The CRO should gain approval and endorsement for these high-level plans or should adjust them in light of suggested changes.

Lecture

05

ERM Review Planning

- ***Risk Management Group*** should establish a strong understanding of the higher risk areas that are within their defined scope and develop risk management project plans for these enterprise risk areas.
- This is the process of defining risk likelihood and criticality.
- ERM function needs to develop a monitoring or review approach.

Lecture
05

ERM Review Planning

- Based on its estimate of the higher likelihood and higher loss probability risk areas, the enterprise risk management function should monitor and review risk areas taking the following approaches:
 - Initiate immediate action to resolve the risk.
 - Review the risk area and propose corrective actions to reduce risk exposures.
 - Arrange with internal audit to perform a review of a selected risk area.
 - Monitor the risk area on a continuous basis.
 - Develop plans to take action only in the event of a risk occurrence.

Lecture

05

ERM Review Planning

- ***Risk Management*** should develop an annual risk assessment action plan.
- Such a time plan would assign responsibilities for the coverage of various risk events, estimate the enterprise risk group's time to correct and review, and include some time and budget estimates.
- The plan should be reviewed and approved by senior management.
- When others such as internal audit are expected to complete portions of the action plan, these events should be coordinated.

Lecture
05

Annual Risk Action Plan Example

Global Computer Products ERM Group Plans—Fiscal Year 2012

Operating Division	Planned Risk Assessment Activity	Responsibility	Planned Actions	Start Date	Due Date	Estimated Remediation Costs
Product Dev.	New Product Security Risks	ERM & IT	Corrective Action Plan			
Product Dev.	India Computer System Operations	ERM	Review			
Product Dev.	Key Documentation Controls	ERM & IA	Corrective Action Plan			
Finance	Vendor Agreements	ERM	Review			
Finance	Staff Risk Management Training	ERM & HR	Implement			

Risk Management Policies, Standards, and Strategies

Lecture

05

Implementing ERM in the Enterprise

PMG 611
Enterprise Risk Management

Lecture

05

Risk Management Policies, Standards, and Strategies

- The ***Risk Management Function*** must encompass all enterprise units and levels.
- The ERM function must be managed and communicated to a wide group of responsible persons throughout the enterprise.
- There are needs to develop some risk management policies and standards that are followed by units in the enterprise, following a consistent strategy.
- Designated managers throughout the enterprise should be trained on these risk management policies and then charged with their implementation.

Lecture

05

Risk Management Policies, Standards, and Strategies

- The point here is that while enterprise risk should be managed and directed by a central CRO-led function, responsibilities and tasks need to be pushed down and across the enterprise by building a **risk-sensitive culture** throughout the enterprise.
- Stakeholders at all levels need to be aware of some of the risks that the enterprise is facing, the consequences of those risk exposures, and some of the steps they can put in place to limit those risks.

Lecture

05

Risk Management Policies, Standards, and Strategies

- Some of the steps necessary to build and implement an effective risk management culture:
 - ***Build a Risk-Awareness Culture.***
 - The “tone at the top”
 - ***Creating the Enterprise-Wide Risk Management Organization.***
 - Professional staff (a good understanding of the risks impacting the enterprise, techniques for limiting risk exposures).
- ***Enterprise Risk Management Policies and Standards.***

Lecture

05

Risk Assessment Sign-Off Acknowledgment Form

- The purpose of such a risk assessment signoff form to encourage all stakeholders to acknowledge that they have considered risks when authorizing and approving a financial transaction above some designated value.



Global Computer Products

Risk Assessment Acknowledgment

Operating Unit _____ Responsible Manager _____ Date ____

Activity Description _____ Asset Value _____ Cntl # ____

If greater than guidelines, was activity sent to Enterprise Risk for review? _____

For qualifying other activities, were risks reviewed by operating unit? _____

I have assessed the operational and financial risks associated with the activity
and have taken appropriate actions per Risk Guidelines.

Risk Acknowledgment Signature _____

Risk Management Reviews and Corrective Action Practices

Lecture

05

Implementing ERM in the Enterprise

PMG 611
Enterprise Risk Management

Lecture

05

Risk Management Reviews and Corrective Action Practices

- **Risk Assessment Reviews (RARs)** should examine key areas in the enterprise and make recommendations for both improving internal controls and reducing risk likelihoods.
- The **Risk Management Group** should develop such a review approach, communicating their review plans and procedures with senior management, internal audit, and the board audit committee.

Lecture

05

Risk Management Reviews and Corrective Action Practices

- **RAR** reviewers would emphasize a wide range of identified risks in the area selected and then would suggest approaches to eliminate or minimize these risks.
- the **Enterprise Risk Reviewers** should form a standard set of review steps to review the identified area.

The following outlines the steps necessary to perform a risk assessment review (RAR) in compliance with the COSO ERM framework:

1. Schedule review based on long-range risk assessment plans, management request, or unanticipated risk event.
2. Develop preliminary objectives for the RAR:
 - a. Review current risk status for management reporting.
 - b. Risk-related assessment in conjunction with internal audit or other group.
 - c. Perceived enterprise risk exposure in area to be reviewed.
3. Review supporting data to gain understanding nature of risk, its severity, occurrence probability, and alternatives for risk mitigation.
 - a. Review supporting data or perform tests of data to better understand the nature of deviations or further risks of occurrence.
 - b. Reconcile results of reviews with preliminary risk assessment objectives.
4. Develop cost-based alternative risk mitigation strategies, such as risk substitution or risk acceptance.
 - a. Review mitigation strategies with responsible management to assess feasibilities.
 - b. Develop best approaches for risk mitigation.
 - c. When practicable, test proposed mitigation strategies.
5. Develop exit strategy for RAR.
 - a. Recommendations for immediate corrective action to be performed by operating unit.
 - b. Corrective actions to be performed through a planned scheduled project.
 - c. Corrective remediation performed by the ERM team.
 - d. Documented avoidance of risk.
6. Publish RAR with copies to responsible management, the risk committee, and a request for RAR wrap-up actions at a designated date.

Lecture

05

RAR Sample Review Guidance



Governance & Culture

1. Exercises Board Risk Oversight
2. Establishes Operating Structures
3. Defines Desired Culture
4. Demonstrates Commitment to Core Values
5. Attracts, Develops, and Retains Capable Individuals



Strategy & Objective-Setting

6. Analyzes Business Context
7. Defines Risk Appetite
8. Evaluates Alternative Strategies
9. Formulates Business Objectives



Performance

10. Identifies Risk
11. Assesses Severity of Risk
12. Prioritizes Risks
13. Implements Risk Responses
14. Develops Portfolio View



Review & Revision

15. Assesses Substantial Change
16. Reviews Risk and Performance
17. Pursues Improvement in Enterprise Risk Management



Information, Communication, & Reporting

18. Leverages Information and Technology
19. Communicates Risk Information
20. Reports on Risk, Culture, and Performance

Summary

Lecture

05

Implementing ERM in the Enterprise

PMG 611
Enterprise Risk Management

- Those *Risk Management Functions* were not structured at a senior or C-level status in enterprise charts.
- An effective *Risk Management Function* would be headed by a *Chief Risk Officer (CRO)*
- An executive whose responsibility is to ascertain that *enterprise risks* are properly *understood* and *translated* into meaningful
 - *business requirements*
 - *Objectives*
 - *metrics.*

- An enterprise *Risk Management Analyst* reviews the potential new product liability risks in a given business area.
- *Risk Management Function* may identify governmental actions that may place some foreign country operations at risk.
- An *Enterprise Risk Management Specialist* with strong IT skills may access system vulnerabilities in what is often called a firewall perimeter surrounding an area of IT operations.

Take
Actions



Risk Activity Scope

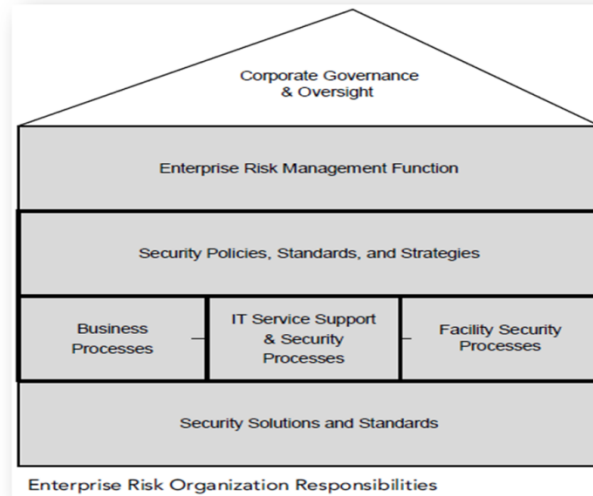
Global Computer Products

The corporate Enterprise Risk Management (ERM) group is responsible for monitoring and developing remediation plans for all major corporate operational risks. Operational risks include, but are not limited to, all major activities involving the development of new company products, acquisition and maintenance of assets, legal and regulatory issues, financial reporting, and internal controls. The ERM group will establish guidelines for all risk management processes, will assign the management of some risks to appropriate operating units, but will assume the direct management of others.

ERM recognizes there are some market, economic, or environmental risks that are beyond its scope and ability to take corrective actions. ERM will communicate these risk issues with the board of directors' risk committee and will assist in risk remediation where appropriate.

Roles and Responsibilities of an Enterprise Risk Management Function

- Whether a relatively small organization or a multidivisional, multicounty type of enterprise, any risk management function should follow these same general operational standards and guidelines.



Risk Assessment Sign-Off Acknowledgment Form

- The purpose of such a risk assessment signoff form to encourage all stakeholders to acknowledge that they have considered risks when authorizing and approving a financial transaction above some designated value.



Risk Assessment Acknowledgment

Global Computer Products

Operating Unit _____ Responsible Manager _____ Date _____

Activity Description _____ Asset Value _____ Cntl # _____

If greater than guidelines, was activity sent to Enterprise Risk for review? _____

For qualifying other activities, were risks reviewed by operating unit? _____

I have assessed the operational and financial risks associated with the activity and have taken appropriate actions per Risk Guidelines.

Risk Acknowledgment Signature _____

Annual Risk Action Plan Example

Global Computer Products ERM Group Plans—Fiscal Year 2012

Operating Division	Planned Risk Assessment Activity	Responsibility	Planned Actions	Start Date	Due Date	Estimated Remediation Costs
Product Dev.	New Product Security Risks	ERM & IT	Corrective Action Plan			
Product Dev.	India Computer System Operations	ERM	Review			
Product Dev.	Key Documentation Controls	ERM & IA	Corrective Action Plan			
Finance	Vendor Agreements	ERM	Review			
Finance	Staff Risk Management Training	ERM & HR	Implement			

References

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



Thank You