

PMG 611

Enterprise Risk Management

Prepared by Dr. Abdullah Jameel Halawany

جامعة الجميع الذكية

تسعى لتكون الكيان الأول الذي يتبنى مبدأ المجتمع التعليمي
التعاوني ويقدم العلم مقابل العمل لتنمية وبناء المجتمعات.

Lecture 11

Establishing an Effective GRC
Culture throughout the Enterprise



جامعة الجميع الذكية
EVERYONE'S SMART UNIVERSITY

Lecture 11

Session Outline

First Steps to Establishing a GRC Culture



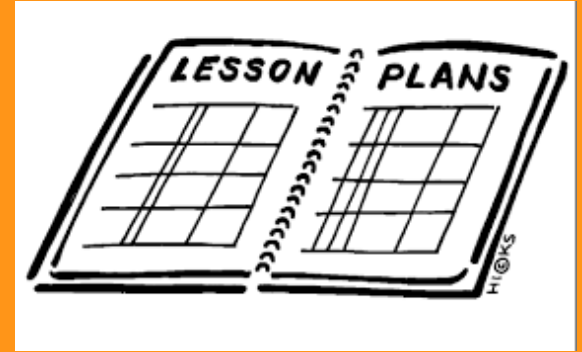
Promoting the Concept of Enterprise Risk



Enterprise Codes of Conduct



GRC Education Programs



Lecture 11

Introduction



جامعة الجميع الذكية
EVERYONE'S SMART UNIVERSITY

- **Enterprise Senior Officers** and **Board Members** often talk among themselves about the importance of launching some new enterprise-wide cultural approach or strategic direction.
- That type of new approach, however, will not launch new products in the marketplace or open new facilities.
- It is also a concept that will be just talk until it is properly communicated to and accepted by all stakeholders in the enterprise.

- The matter or issue must become part of the enterprise's “*Culture*”.
- A concept that sounds good but is difficult to execute.
- Some enterprises, due to their many frequent changes, have never been able to establish a recognized culture, while others have built enduring cultures over the years.

- Culture refers to an enterprise's values, beliefs, and behaviors.
- In general, it forms the basis on which people interpret experiences and behave, individually and in groups.
- Enterprises with strong cultures generally achieve higher results because employees sustain their focus on both what to do and how to do it.
- These same factors are also **essential for building** an **effective governance, risk management, and overall compliance culture** in an enterprise.

- Whether the chief executive officer (CEO) and board have **indicated** that *the enterprise wants to grow rapidly and are willing to take necessary steps to get there* **or** they have *indicated a strategy of cautious steps for new ventures*, they are *describing their culture and outlining a high-level risk strategy*.

- In order to get an enterprise operating in either manner, these concepts should be communicated to become part of the overall enterprise-wide culture.
- That is, if a rapid growth strategy is planned, managers and staff at all levels need to think and make decisions to help promote that rapid growth.
- *They are building a culture of growth for the enterprise!*

- That same concept is necessary to build an effective GRC culture in an enterprise.
- This should be a culture that reflects the ***appetite for risk*** that has been described and defined by senior management, that has strong standards for regulatory and rules compliance, and that has an overall *governance program* that should be *followed by stakeholders at all levels*.

Lecture 11

First Steps To Establishing A GRC Culture



جامعة القصيم الذكية
EVERYONE'S SMART UNIVERSITY

- *Enterprises worldwide are starting to take corporate governance, risk, and compliance seriously.*
- There is growing awareness among organizations of the risks of not having such a program in place.
- Because every enterprise is unique, there is no “**one size fits all**” approach toward implementing a successful GRC framework.
- There are several common challenges enterprises face when developing and implementing an effective GRC strategy and overall culture.

- General GRC concepts and concerns must be clearly communicated and understood by all enterprise stakeholders, whether employees, vendors, or others.
- This can be a difficult concept for many.
- While there is usually a general understanding as to the meaning of the terms governance, risk, and enterprise compliance, many will have problems translating these concepts in any greater level of detail or action plans.

- Enterprises need to build and establish strong GRC cultures that are understood and implemented throughout their operations and on a continuous ongoing basis.
- ***How to build an enterprise-wide GRC culture?***
 - Developed and Released a Revised Employee Code of Conduct.
 - Launched a Strong Program of Ethics Education.
 - Revised and Rewrote Many Existing Policies and Procedures.
 - Established a Whistleblower Program.

- *Developed and Released a Revised Employee Code of Conduct.*

- A revised set of code of conduct rules should be developed, released, and communicated through strong enterprise-wide code of ***conduct educational programs***.
- After strong CEO and other senior management endorsements, employees have to be asked to formally acknowledge that they had read these code of conduct rules, understood them, and would follow them.

- *Launched a Strong Program of Ethics Education.*

- Through company classes, articles in newsletters, posters, and ongoing communications from senior managers, the message to always “***Do The Right Thing***” must be communicated to all stakeholders.
- The idea is to reinforce the idea of being ethical into the culture of the enterprise.

- *Revised and Rewrote Existing Policies and Procedures.*
 - Examination of the entire set of enterprise's policies and procedures.
 - Put in place a processes to better review and communicate these “*New Rules*”.
- *Established a Whistleblower Program.*

Lecture 11

Promoting The Concept Of Enterprise Risk



جامعة الجميع الذكية
EVERYONE'S SMART UNIVERSITY

- Risk management is one of the three important GRC principles.
- Perhaps a tough sell to begin, the concept and importance of risk management needs to be communicated and constantly promoted to all members of the enterprise.
- In a very subtle way, this idea of building a risk awareness culture is a bit more difficult than promoting an ethics culture.

- With *Ethics*, it is often sufficient to encourage employees to “do the right thing” with a shared value that most understand enough of right and wrong to easily make decisions.
- Risk management too often involves some “shades of gray” concepts where an enterprise may have an appetite for either high or low levels of risk, and with stakeholder decisions based on that philosophy.

- Mutual understanding of the enterprise risk culture is important!
- An enterprise needs to clearly define its risk management philosophy in a manner that can be understood at all levels.
- Communicating a risk management philosophy can be difficult because there are always shades of variability in any enterprise's approach to managing its risks.

- In many respects, drafting such a formal GRC philosophy statement is similar to developing any high-level statement, such as a management objective or a code of conduct.
- In a precise and explicit way, these statements and messages must express a risk management philosophy in a clear and succinct manner.

- Depending on the talents and skills within the enterprise, drafting such published statements may require the talents and skills of specialized people in the enterprise or through outside contracted help.
- Considerable care must be given to the nature of the message in that philosophy.

- It must emphasize that there are risks associated with all business transactions and that stakeholders must make decisions that are consistent with the enterprise's risk philosophy.



Global Computer Products

Our Governance, Risk, and Management Philosophy Compliance Policy

Governance, risk, and compliance (GRC) management is not just a process or procedure. It is a fundamental component of Global Computer Products' business. Our company is dedicated to keeping GRC management issues as key components of all of our business dealings.

We believe that overall GRC management is first and foremost the responsibility of all associates, including management up to the most senior level. Just as a successful business must manage its costs, it must manage its risks. This includes hazard risk, financial risk, and credit risk.

The management of governance, risks, and compliance with rules must be incorporated into the fiber of our organization. All associates must understand established rules and procedures; comply with rules, laws and regulations; and consider potential risks as they make all decisions, whether in sales, product development, or other areas of operations.

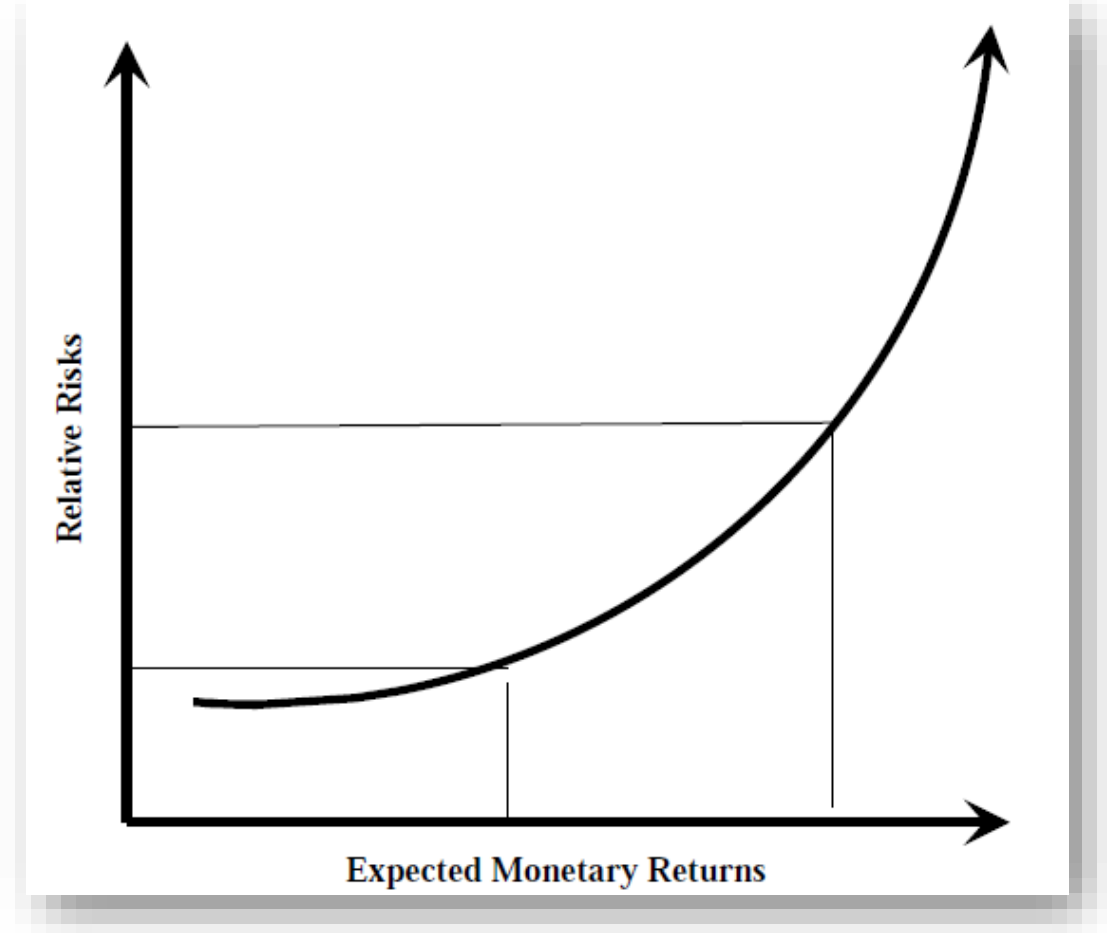
- Stakeholders need to understand any such statement and to take active steps to implement it in their day-to-day business activities.
- They need to understand that all activities involve some risks, but their activities should be consistent with that philosophy.

- 3M Corporation is a good example of a company where stakeholders at all levels were encouraged to try new products or ventures to build the business.
- Not every new venture worked, but the team there has evidently been encouraged over the years to take some prudent risks in order to encourage strong growth patterns.
- This appears to be an environment where some risk appears to be tolerated in order to achieve growth.

Lecture 11

Translating a Risk Philosophy into a Culture

- Too much of a high-risk culture with poor governance procedures is usually not good.
- Both of extremes of very high - or very low-risk approaches are the results of fairly deliberate management strategies that should be understood by stakeholders.



Relative Risks versus Expected Returns

Lecture 11

Translating a Risk Philosophy into a Culture

- Repeat Higher-Risk or Lower-Risk Strategies in All Business Communications.
- Understand the Rules and Take Appropriate Compliance Actions..
- Clearly Reward People for Making Appropriate Risk-Based Decisions.
- Encourage All Stakeholders to Follow Good GRC Policies and Procedures.

Lecture 11

Enterprise Codes Of Conduct



جامعة الجميع الذكية

EVERYONE'S SMART UNIVERSITY

- While a mission statement is a keystone to hold together the overall structure of corporate governance, an effective code of conduct provides the supporting rules for enterprise stakeholders.
- An enterprise today should develop and enforce a code of conduct that covers a set of appropriate ethical, business, and governance rules for all of its stakeholders, whether the financial officers, all other employees, or a larger group of stakeholders.

- An effective **Code Of Conduct** will promote ethical business and GRC practices throughout an enterprise.
- It is a key component of an enterprise's GRC culture.
- A **Code Of Conduct** should be a clear, unambiguous set of rules or guidance that outlines rules or what is expected of members of the enterprise, whether officers, employees, contractors, vendors, or other stakeholders.
- The **Code** should be both based on the values and legal issues surrounding an enterprise.

- *"During working hours, employees are only permitted to use technology such as cellphones, social media or the internet for personal use while on break."*
- *"Our company's dress code is laid back most days. Employees are free to wear jeans, t-shirts, sweatshirts and leggings that are not see-through. Of course, if employees wish to wear business casual attire, they are encouraged to do so."*

Lecture 11

GRC Education Programs



جامعة الجميع الذكية
EVERYONE'S SMART UNIVERSITY

- Beyond strong messages to stakeholders, an appreciation of all elements of the GRC program should be communicated through ongoing training programs.
- New stakeholders at all levels should learn that their enterprise faces risks and compliance requirements at all levels.
- They are expected to take appropriate actions to consider those risks and to install corrective actions to guard against them.

- Many enterprises are not large enough nor have the time and resources to develop specialized risk management, compliance, and governance training materials, the message of the enterprise's GRC culture can be ***folded into other training materials*** covering other areas.



Global Computer Products

Understanding Risk Management Continuing Education Course Outline

This Web-based risk training will be offered to all members of the Global team.

1. Introduction to enterprise governance, risk, and compliance management.
 - a. Global's GRC management philosophy and a message from the CEO.
 - b. The COSO ERM framework and how it fits.
2. The Global code of conduct and why it is a key component of GRC activities.
3. The risk management team and your ongoing responsibilities.
 - a. Significant new risk-based policies and procedures.
 - b. The Global risk team—the CRO and others.
4. Your company's periodic risk assessment process.
 - a. Updating periodic risk inventories: Updating existing risks and identifying new.
 - b. Responding and reacting to risk assessment reports.
5. Steps for identifying potential new risk concerns.
6. Building compliance and risk remediation strategies into your regular business processes.
7. Case study: Considering GRC issues in new product planning.

Lecture 11

Summary



جامعة الجميع الذكية
EVERYONE'S SMART UNIVERSITY

Lecture 11

- This should be a culture that reflects the appetite for risk that has been described and defined by senior management, that has strong standards for regulatory and rules compliance, and that has an overall governance program that should be followed by stakeholders at all levels.
- A strong ethics program, based on a meaningful mission statement and a code of conduct, are key elements to any overall program of corporate governance in an enterprise.



Global Computer Products

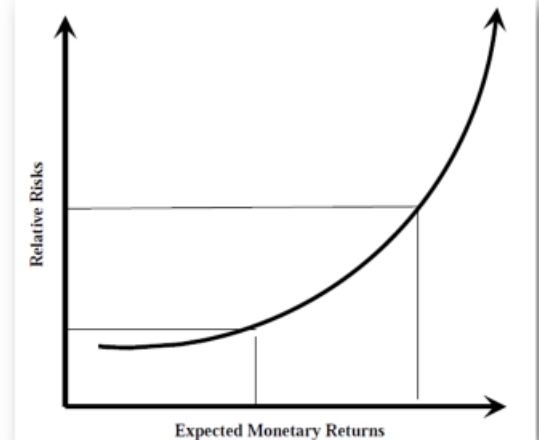
Our Governance, Risk, and Management Philosophy Compliance Policy

Governance, risk, and compliance (GRC) management is not just a process or procedure. It is a fundamental component of Global Computer Products' business. Our company is dedicated to keeping GRC management issues as key components of all of our business dealings.

We believe that overall GRC management is first and foremost the responsibility of all associates, including management up to the most senior level. Just as a successful business must manage its costs, it must manage its risks. This includes hazard risk, financial risk, and credit risk.

The management of governance, risks, and compliance with rules must be incorporated into the fiber of our organization. All associates must understand established rules and procedures; comply with rules, laws and regulations; and consider potential risks as they make all decisions, whether in sales, product development, or other areas of operations.

- Too much of a high-risk culture with poor governance procedures is usually not good.
- Both of extremes of very high - or very low-risk approaches are the results of fairly deliberate management strategies that should be understood by stakeholders.



Relative Risks versus Expected Returns

Lecture 11

References

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



جامعة القصيم الذكية
EVERYONE'S SMART UNIVERSITY