

Enterprise Risk Management

PMG 611

Lecture 4

ERM Frameworks

Prepared by
Dr. Eng. Abdullah Jameel Halawany

Lecture

0

Session Outline

4

Introduction

COSO ERM Framework

ISO 31000:2018

Where's the Value?

Introduction

Lecture

04

ERM Frameworks

PMG 611

Enterprise Risk Management

Lecture

04

Introduction

- Every enterprise, whether for-profit commercial, not-for-profit, or a governmental agency, exists to provide value for its stakeholders.
- That stakeholder value is created, preserved, or even can be eroded through management decisions at all levels of the enterprise and in all of its activities, ranging from day-to-day regular operations to setting strategies for future but uncertain endeavors.
- All of them are subject to uncertainties or risks.

- Over past years, enterprises generally have had two problems with this risk versus adjusted return decision model.
 1. had not been a good and consistently accepted definition of risk across the overall enterprise.
 2. often do not think of risks in a total enterprise sense but usually only on the basis of risk component by component.

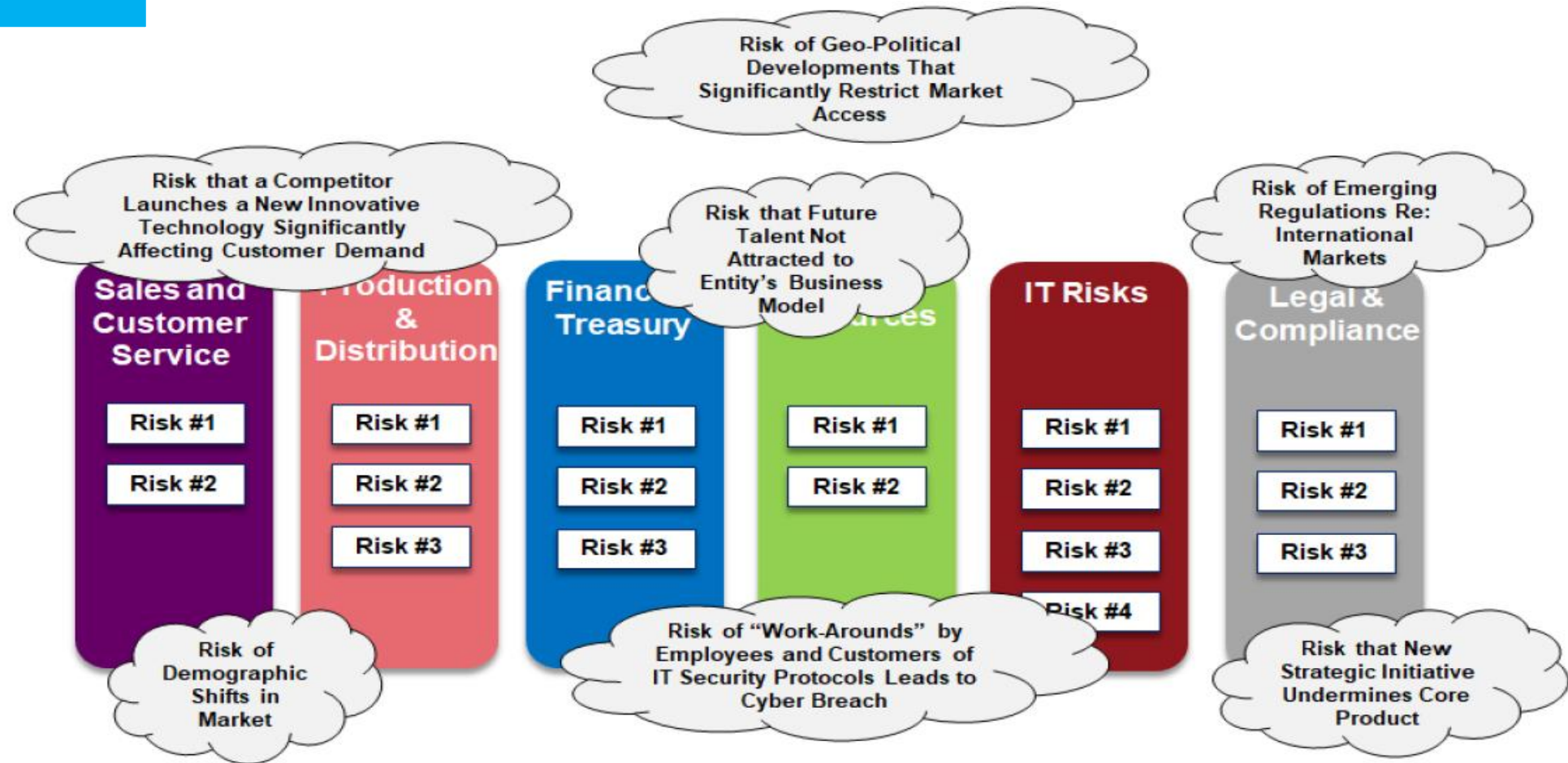
Lecture
04

Traditional Approach to Risk Management



Lecture
04

Currently Unknown, But Knowable Risks Overlooked by Traditional Risk Management



Lecture

04

ERM

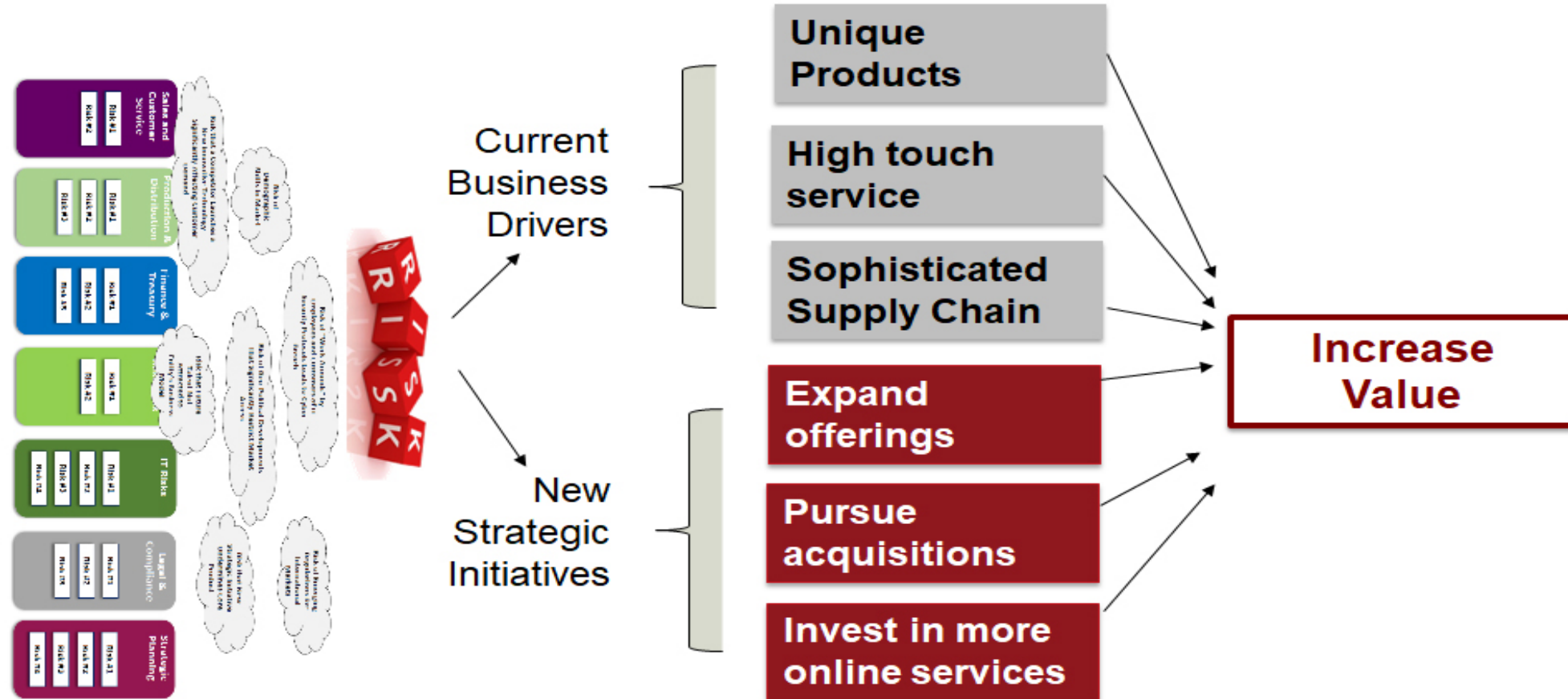
- Provides a comprehensive and systematic approach to more proactive and holistic risk management
- Provides a common lexicon of risk terminology, and provides direction and guidance for implementing ERM
- Requires that organizations examine their complete portfolio of risks, consider how those risks interrelate, and that management develops an appropriate risk mitigation approach to address these risks in a manner that is consistent with the organization's strategy and risk appetite

Lecture

04

ERM

- ERM process begins with a rich understanding of **what's most important** for the business' short-term and long-term success.
- ERM uses a strategic lens to pinpoint emerging risks potentially affecting current core business drives and new strategic initiatives.
- The goal of an ERM process is to generate an understanding of the top risks that management collectively believes are the current most critical risks to the strategic success of the enterprise.



COSO ERM Framework



Lecture

04

COSO Definition for ERM

Enterprise Risk Management (ERM) is defined by the Committee of Sponsoring Organizations (COSO) as

“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**.”

COSO ERM Frameworks

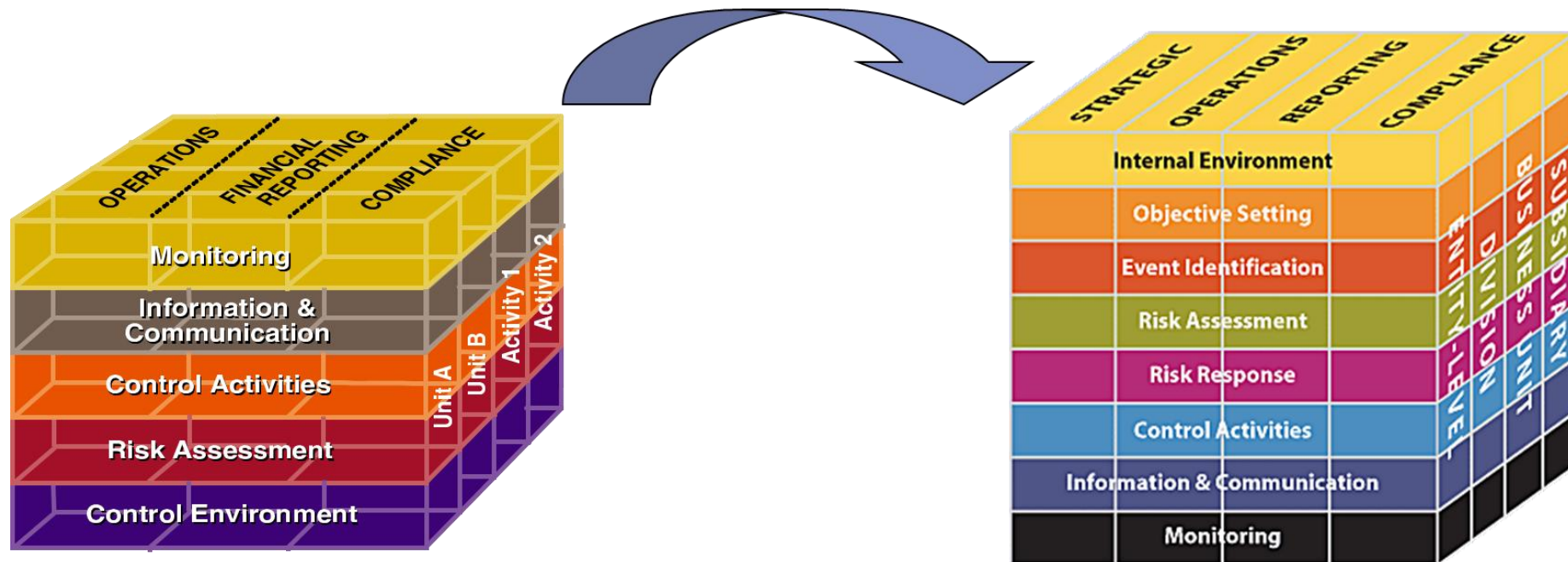


1. Enterprise Risk Management Integrated Framework (2004)
2. Enterprise Risk Management–Integrating with Strategy and Performance (2017)

Lecture
04

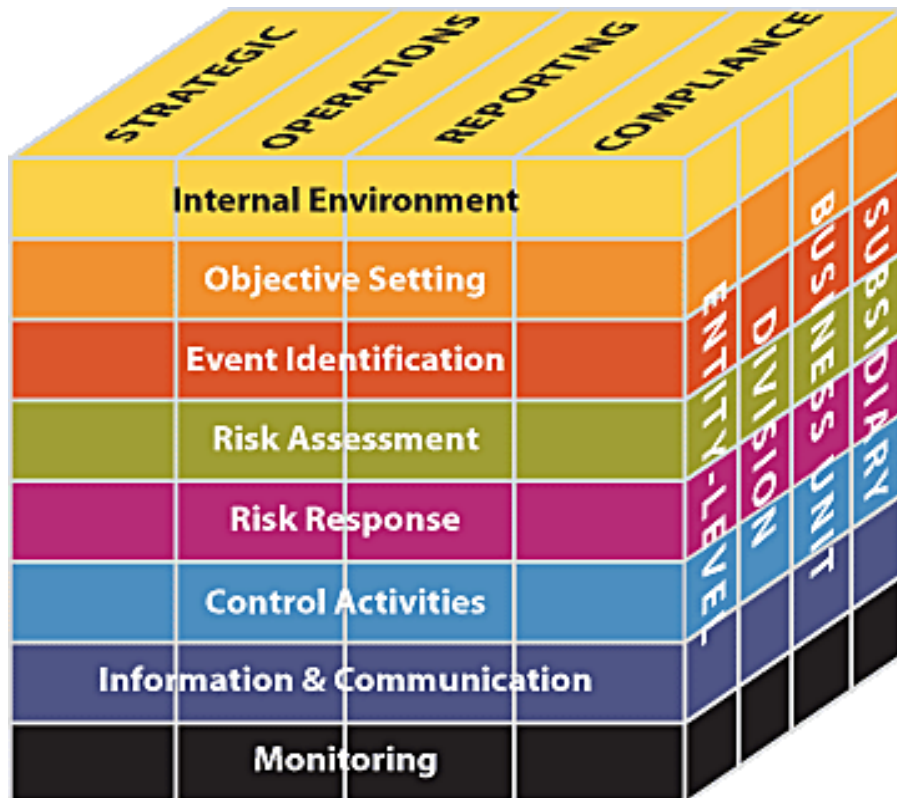
COSO ERM Integrated Framework

To help assist with the implementation of the ERM process, COSO developed the ERM Integrated Framework (2004), also known as the **COSO Cube**. This cube is an update to the initial COSO I framework developed in 1992:



Lecture
04

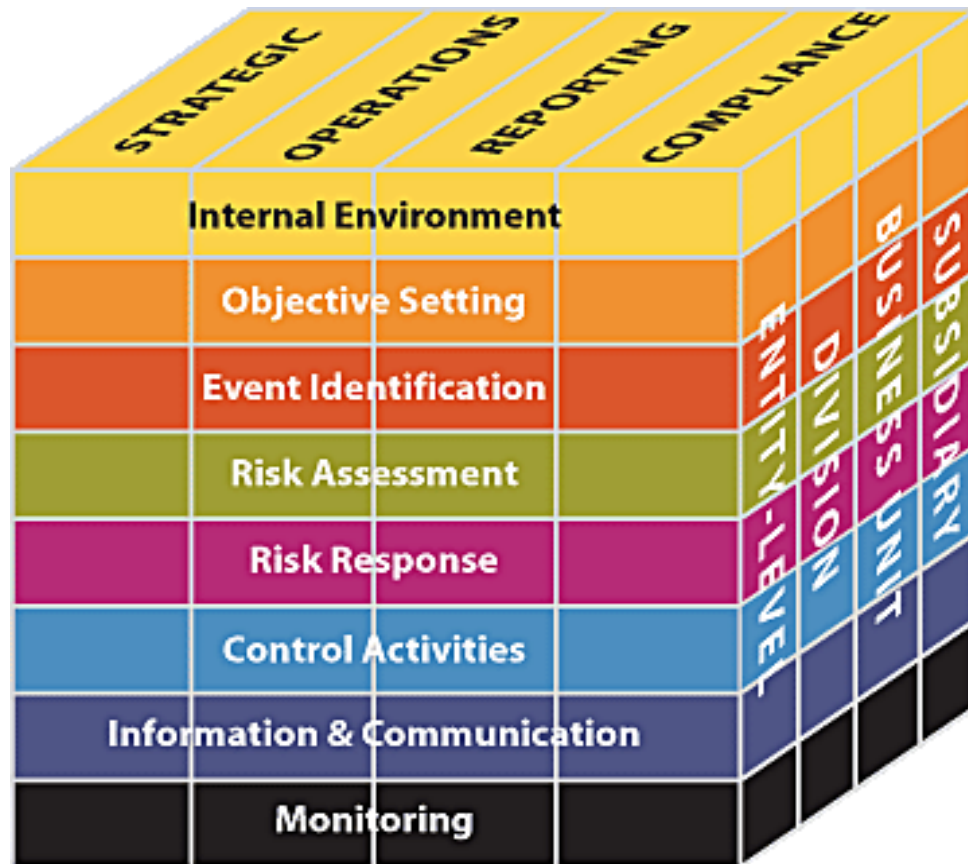
COSO ERM Integrated Framework



These are the high-level goals that are aligned with and support the institution's mission.

Lecture
04

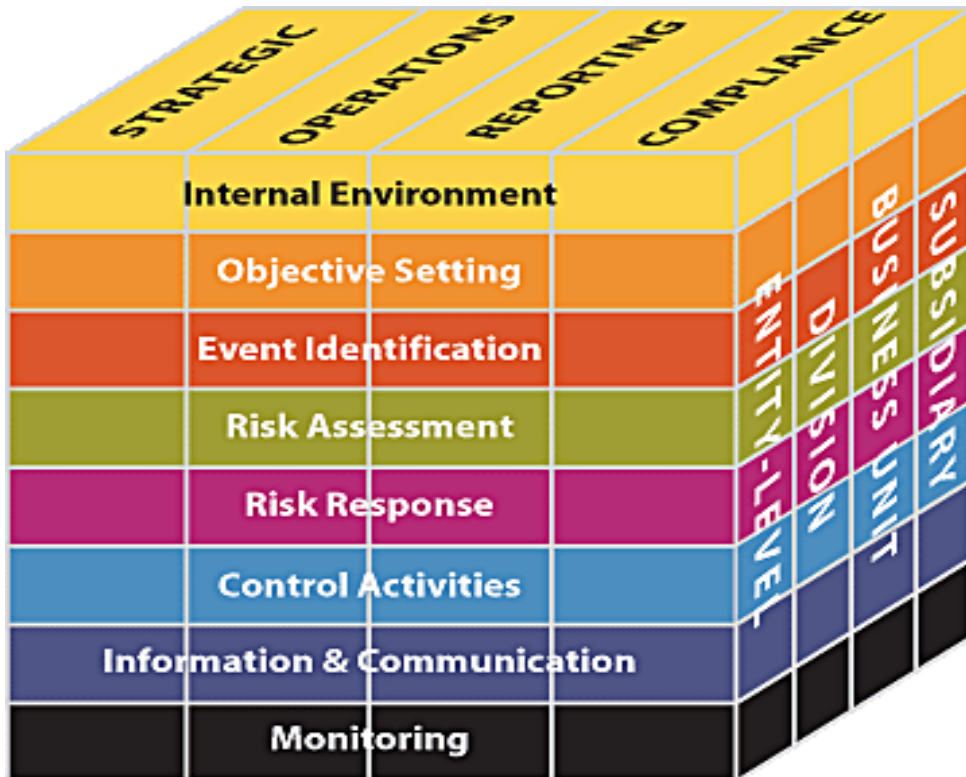
COSO ERM Integrated Framework



Relate to the ongoing management process and daily activities of the organization.

Lecture
04

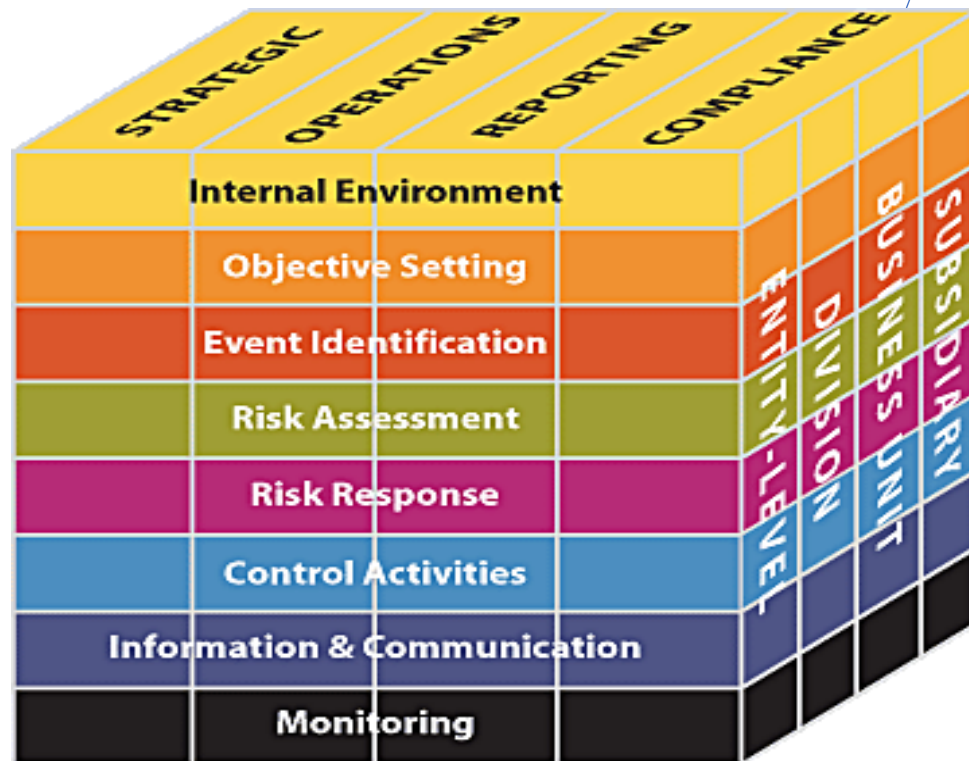
COSO ERM Integrated Framework



Relates to the protection of the organization's assets and quality of financial reporting.

Lecture
04

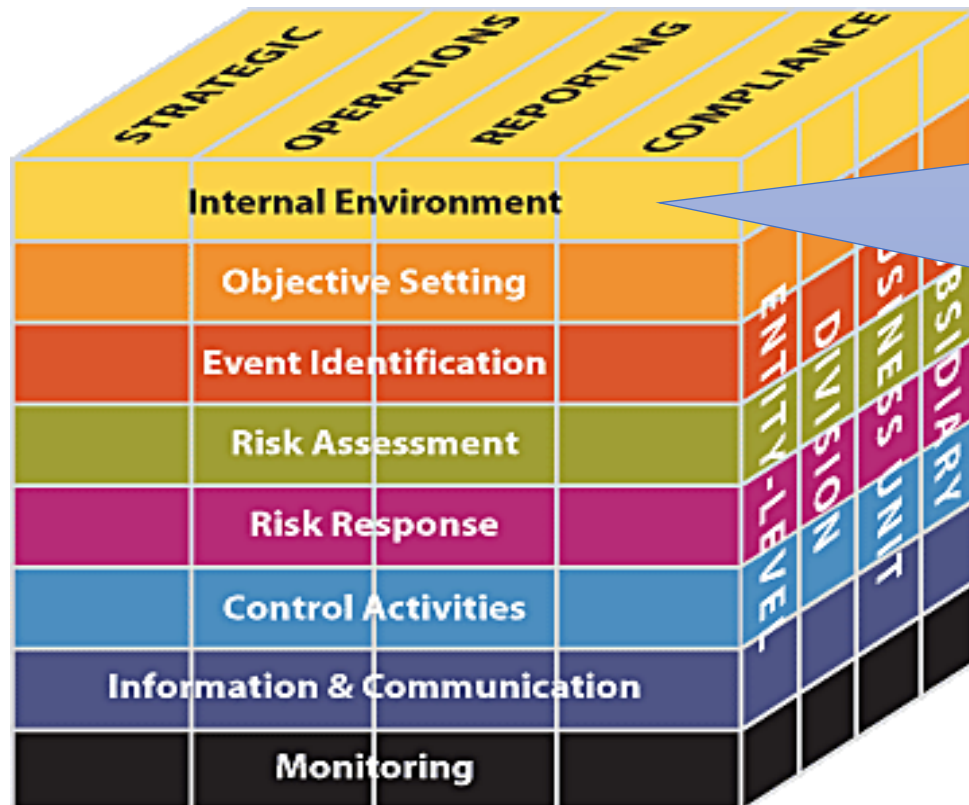
COSO ERM Integrated Framework



Relates to the organization's adherence to applicable laws and regulations.

Lecture
04

COSO ERM Integrated Framework



The Internal Environment relates to the general culture, values and environment in which an organization or entity operates (e.g. – Tone at the top)

Lecture
04

COSO ERM Integrated Framework



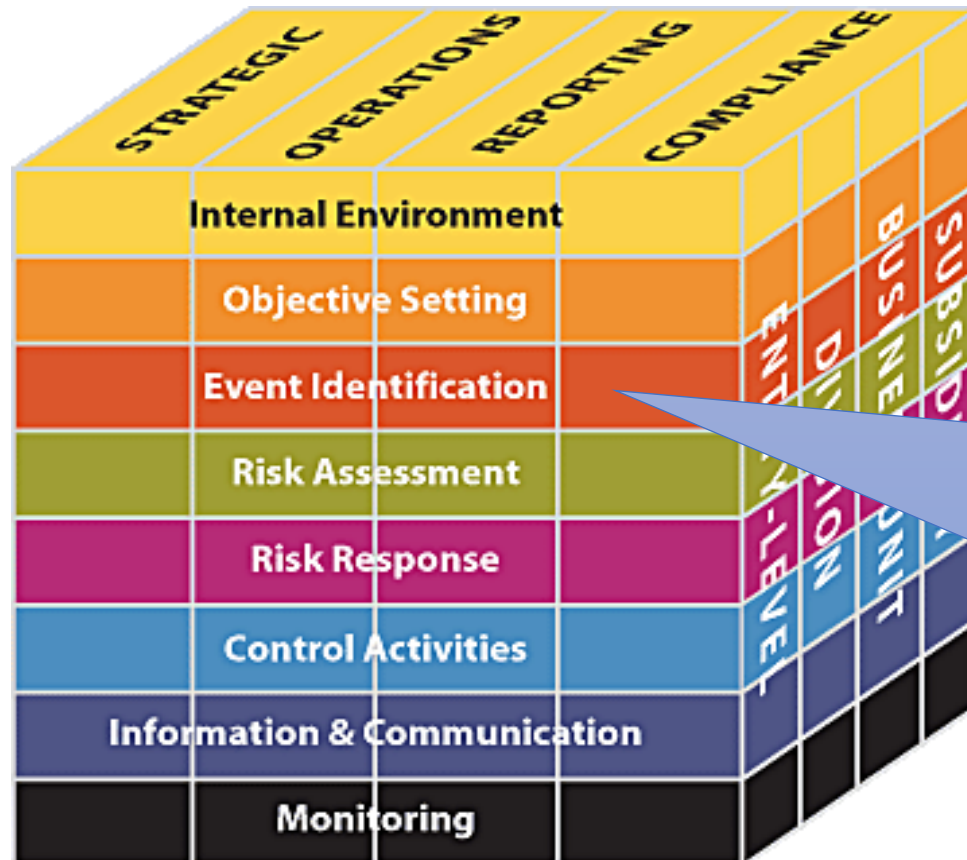
Objective Setting relates to the process management uses to set its strategic goals and objectives. Establishes the organization's risk appetite and risk tolerance.

Risk Appetite is the amount of risk, on a broad level, that an enterprise and its individual managers are willing to accept in their pursuit of value.

Risk Tolerance sets the acceptable minimum and maximum variation levels for a company, business unit, individual initiative, or specific risk category.

Lecture
04

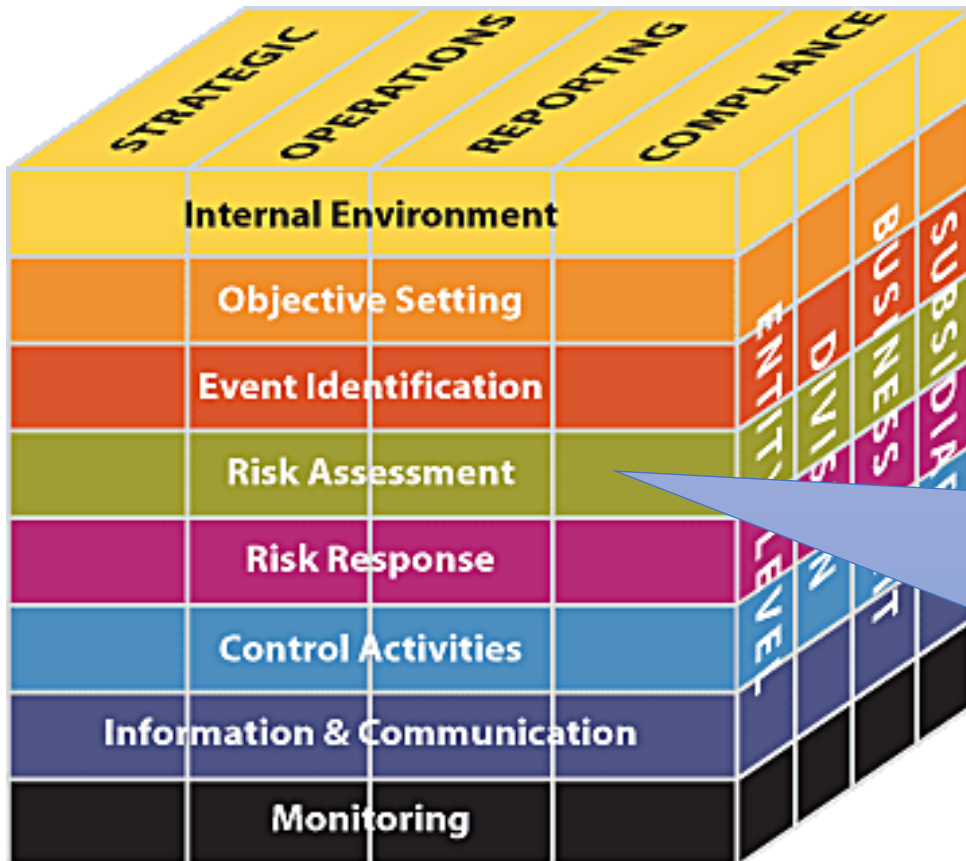
COSO ERM Integrated Framework



Event Identification is the process by which an organization identifies events that influence strategy and objectives or could affect an organization's ability to achieve its objectives.

Lecture
04

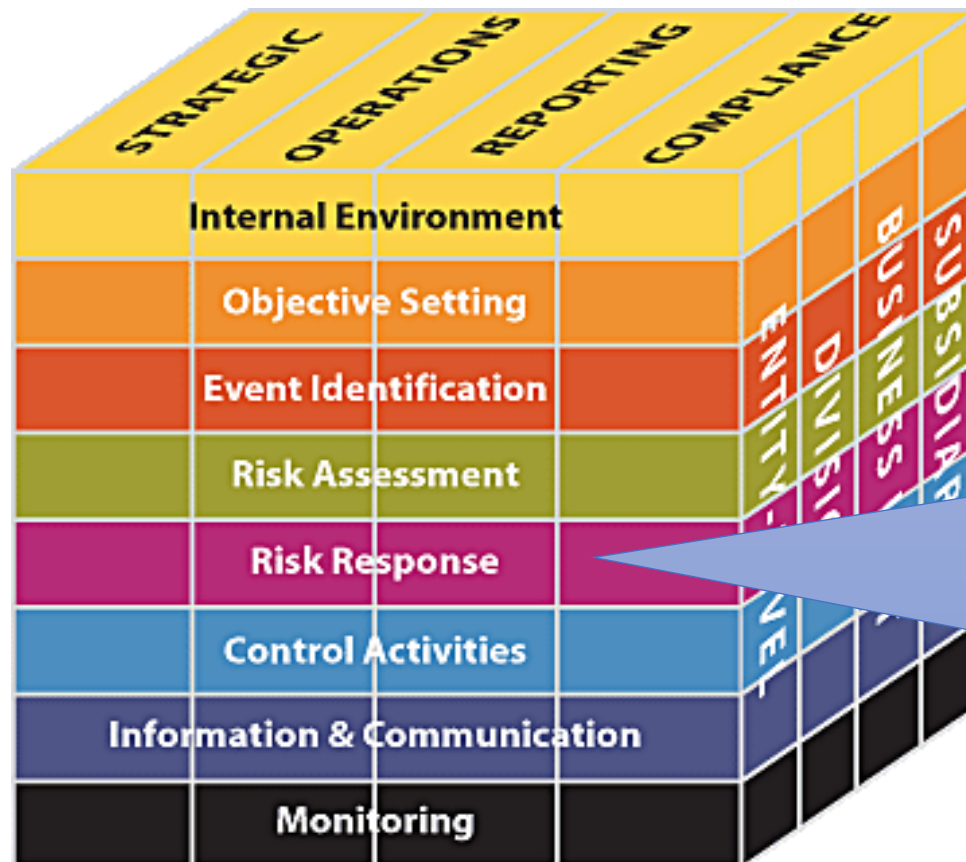
COSO ERM Integrated Framework



Risk Assessment relates to the organization's process of evaluating the impact and likelihood of events and prioritizing related risks.

Lecture
04

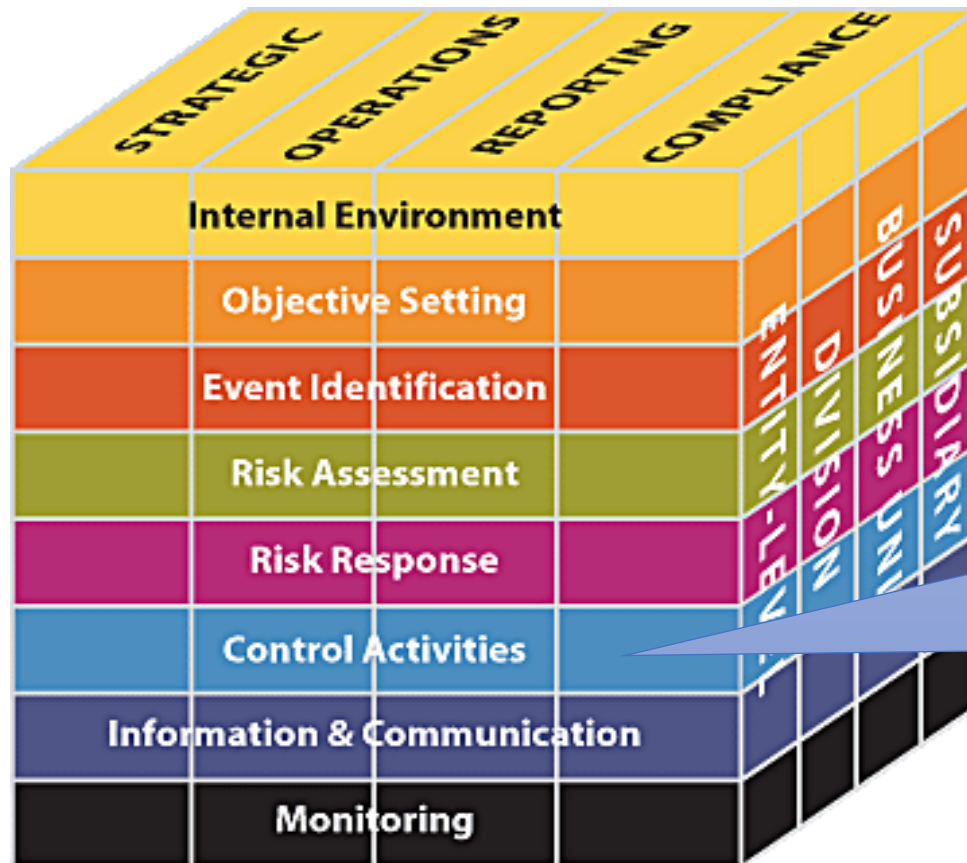
COSO ERM Integrated Framework



Risk Response relates to determining how management will respond to the risks an organization faces. Will they avoid the risk, share the risk, or mitigate the risk through updated practices and policies.

Lecture
04

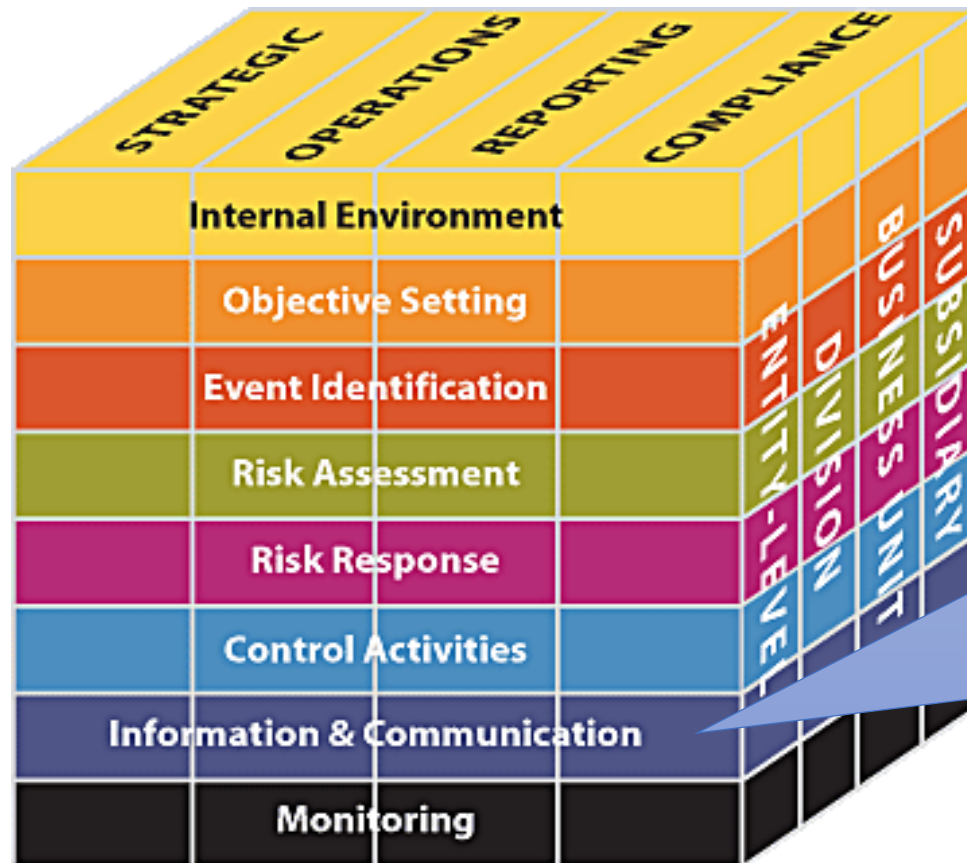
COSO ERM Integrated Framework



Control Activities represent policies and procedures that an institution implements to address the risks the organization chooses to accept.

Lecture
04

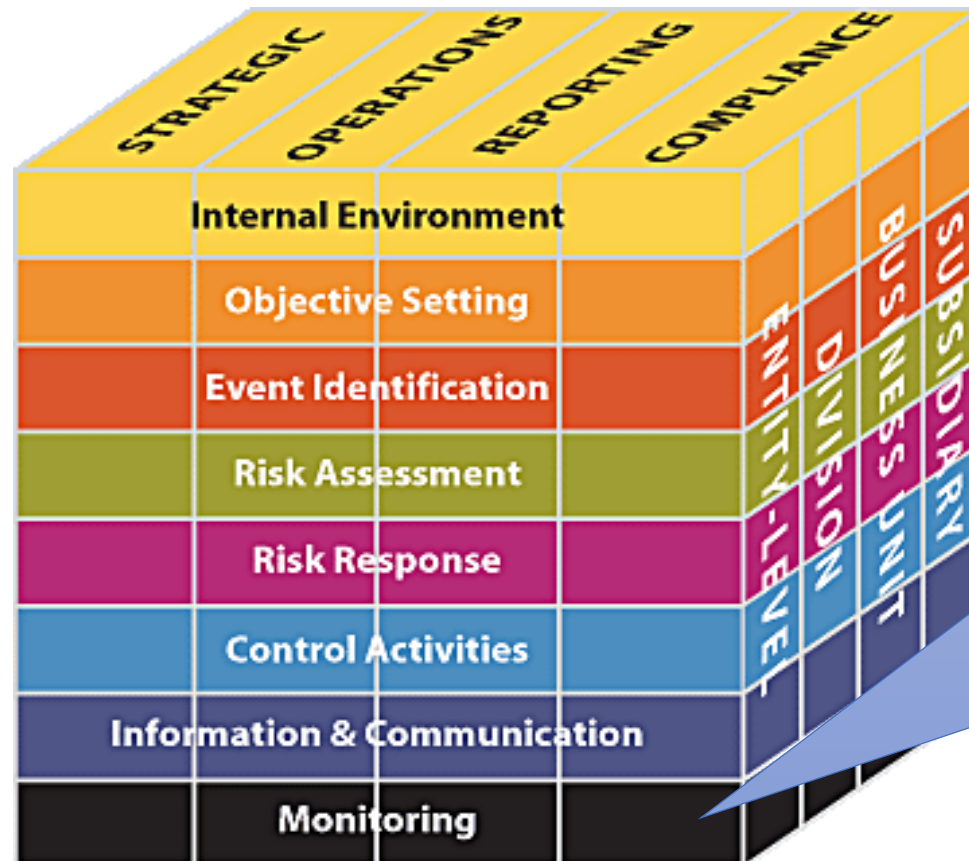
COSO ERM Integrated Framework



Information and Communication relate to those practices that ensure that the right information is communicated at the right time to the right people.

Lecture
04

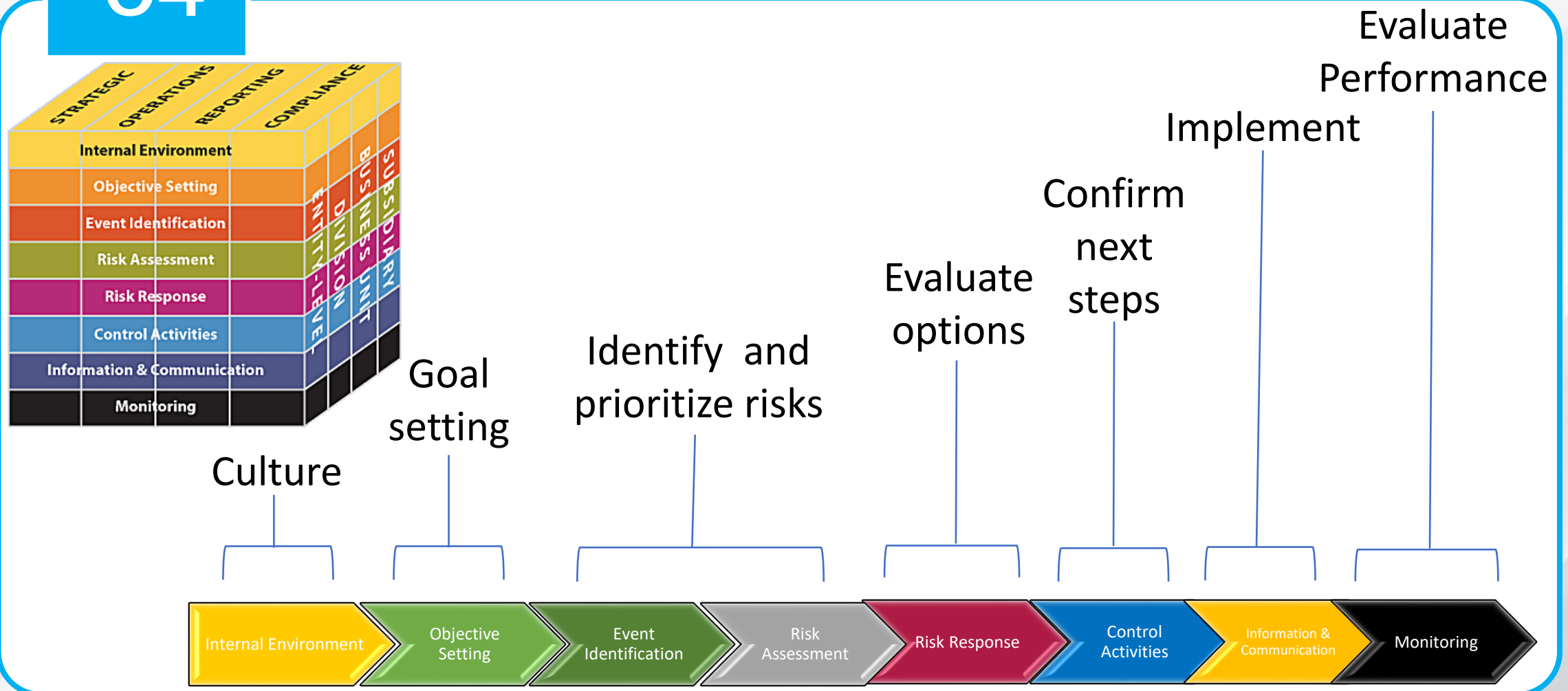
COSO ERM Integrated Framework



Monitoring consists of ongoing evaluations to ensure controls are functioning as designed and taking corrective action to enhance control activities if needed.

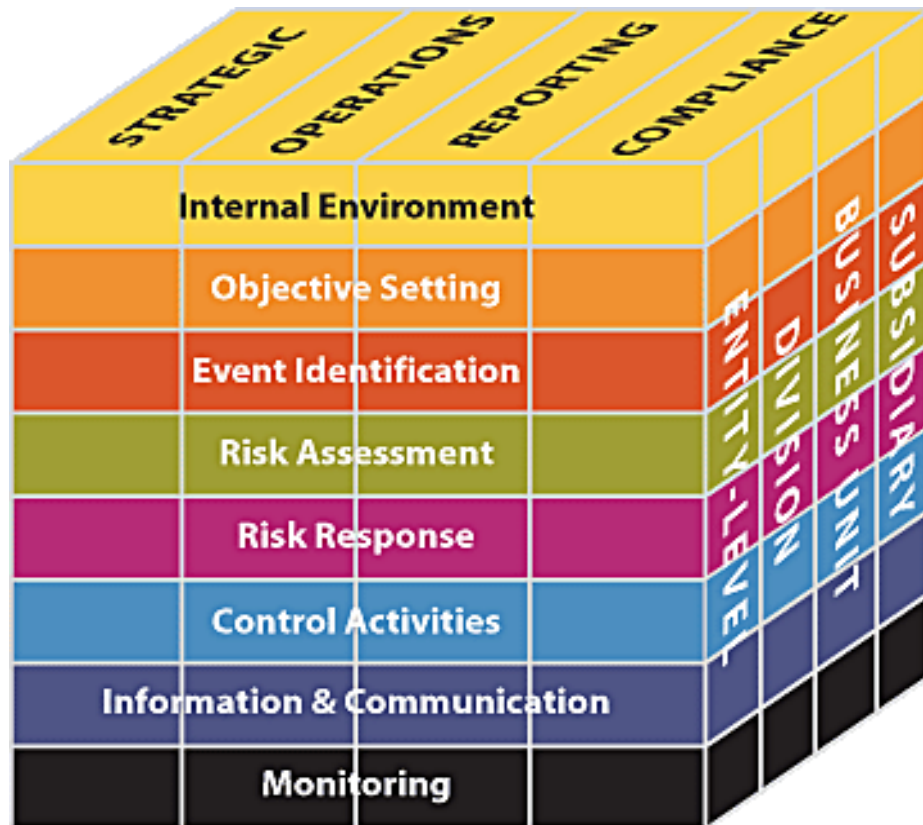
Lecture
04

COSO ERM Integrated Framework



Lecture
04

COSO ERM Integrated Framework



Each of these components are considered at multiple levels of the organization, rather than within a single function, unit, or department.

COSO ERM Frameworks



1. Enterprise Risk Management Integrated Framework (2004)
2. Enterprise Risk Management—Integrating with Strategy and Performance (2017)

Lecture
04

COSO ERM Integrating with Strategy and Performance

- The updated Framework elevates the discussion of integrating strategy and risk through three different dimensions:
1. The possibility of strategy not aligning with mission, vision and core values.
 2. The implications from the strategy chosen.
 3. Risk to strategy and performance.



Lecture

04

COSO ERM Integrating with Strategy and Performance

- The Framework recognizes the importance of enterprise risk management keeping pace with technological developments
 - Emphasizes how enterprise risk management practices and capabilities need to *align with the velocity of changes* to the business context, emerging and changing risks.
 - Information, Communication and Reporting principles now have a greater focus on *integrated risk and performance reporting*.
 - Developments in *data generation and analytics* including ‘big data’, artificial intelligence and social media have been acknowledged.

- Culture now features in the definition of ERM and is part of the Framework's Governance and Culture Component.
- Principles on culture are now more focused on decision-making and the alignment to expected behaviors in line with the core values of the organization

Lecture
04

COSO ERM Integrating with Strategy and Performance



Lecture

04

COSO ERM Integrating with Strategy and Performance

- The Framework itself is a set of principles organized into five interrelated components:

1- Governance and Culture

2- Strategy and Objective-Setting

3- Performance

4- Review and Revision

5- Information, Communication, and Reporting

1- Governance and Culture

- Governance sets the organization's tone, reinforcing the importance of, and establishing oversight responsibilities for, enterprise risk management.
- Culture pertains to ethical values, desired behaviors, and understanding of risk in the entity.

2- Strategy and Objective-Setting

- ERM, strategy, and objective-setting work together in the strategic-planning process.
- A risk appetite is established and aligned with strategy.
- Business objectives put strategy into practice while serving as a basis for identifying, assessing, and responding to risk.

3- Performance

- Risks that may impact the achievement of strategy and business objectives need to be identified and assessed.
- Risks are prioritized by severity in the context of risk appetite.
- The organization then selects risk responses and takes a portfolio view of the amount of risk it has assumed.
- The results of this process are reported to key risk stakeholders.

4- Review and Revision

- By reviewing entity performance, an organization can consider how well the enterprise risk management components are functioning over time and in light of substantial changes, and what revisions are needed.

5- Information, Communication, and Reporting

- Enterprise risk management requires a continual process of obtaining and sharing necessary information, from both internal and external sources, which flows up, down, and across the organization.

Lecture 04

COSO ERM Integrating with Strategy and Performance



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

ISO 31000:2018

Lecture

04

ERM Frameworks

PMG 611

Enterprise Risk Management

- The International Organization For Standardization's (ISO) international standards cover a wide range of areas, ranging from defining the dimensions of fastener screw threads in an automobile engine to the thickness of a personal credit card to information technology (IT) quality standards.
- These standards also have been expanded over the years to cover areas that are important for enterprise governance and quality.

Lecture

04

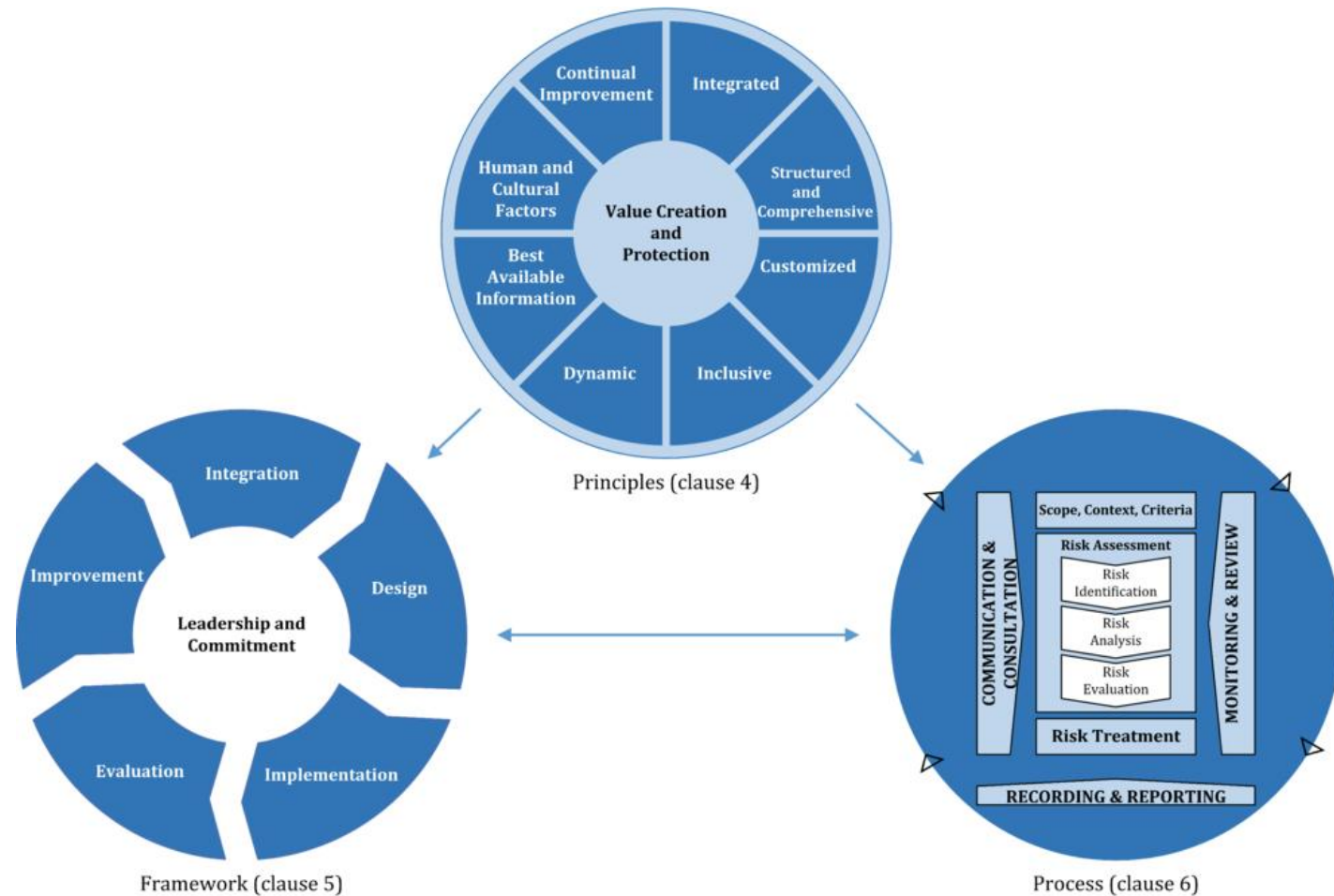
ISO 31000:2018

- The concept behind ISO 31000 is that there are international companies operating in many countries around the globe who all need to set priorities and address risks in a consistent manner.
- There is a need for a “*common look and feel*” for these various countries to demonstrate to outside viewers that effective and reliable standards have been used.
- It should be emphasized that ISO 31000 is not a prescriptive set of rules but a set of principles and generic guidelines.

Lecture
04

ISO 31000:2018

<https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:en>

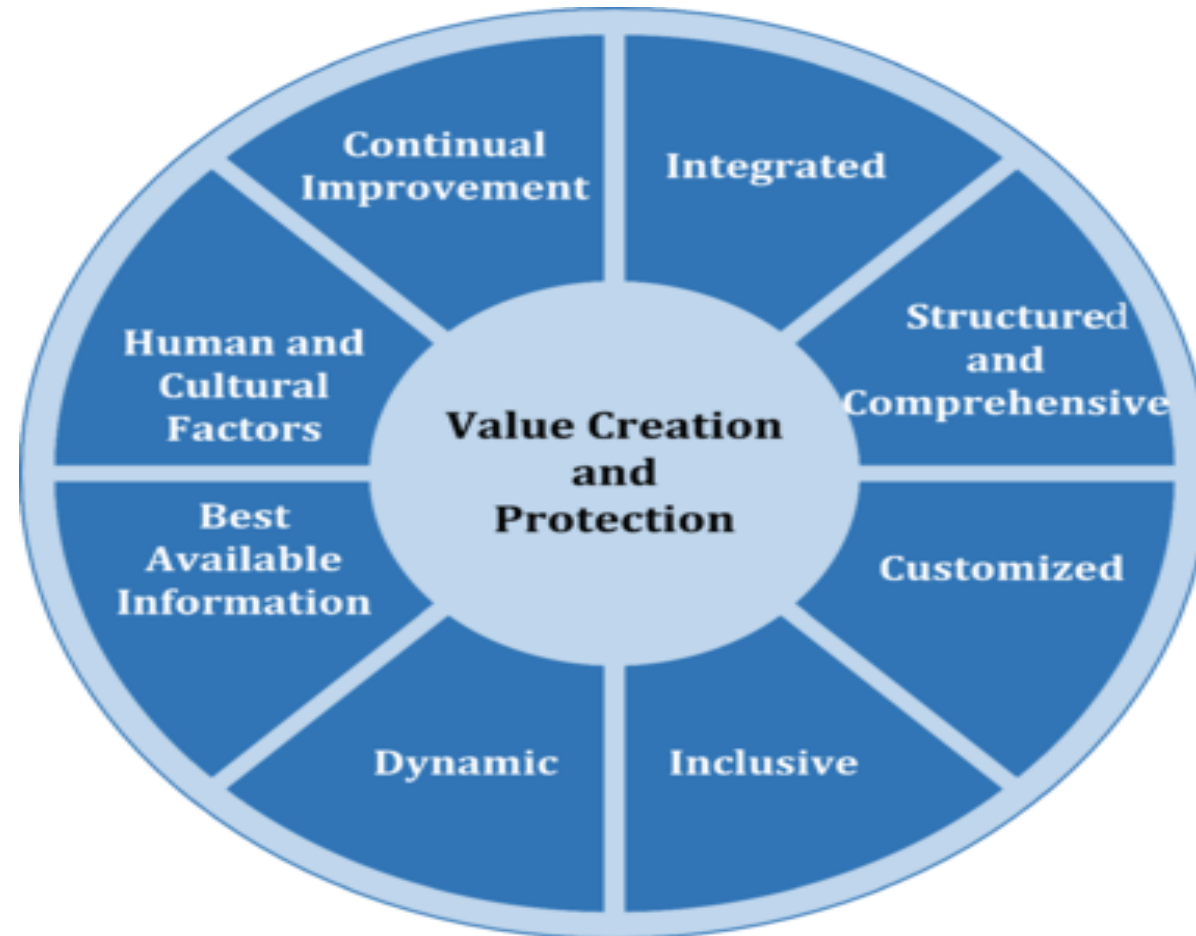


Lecture

04

ISO 31000:2018

Principles



Lecture

04

ISO 31000:2018

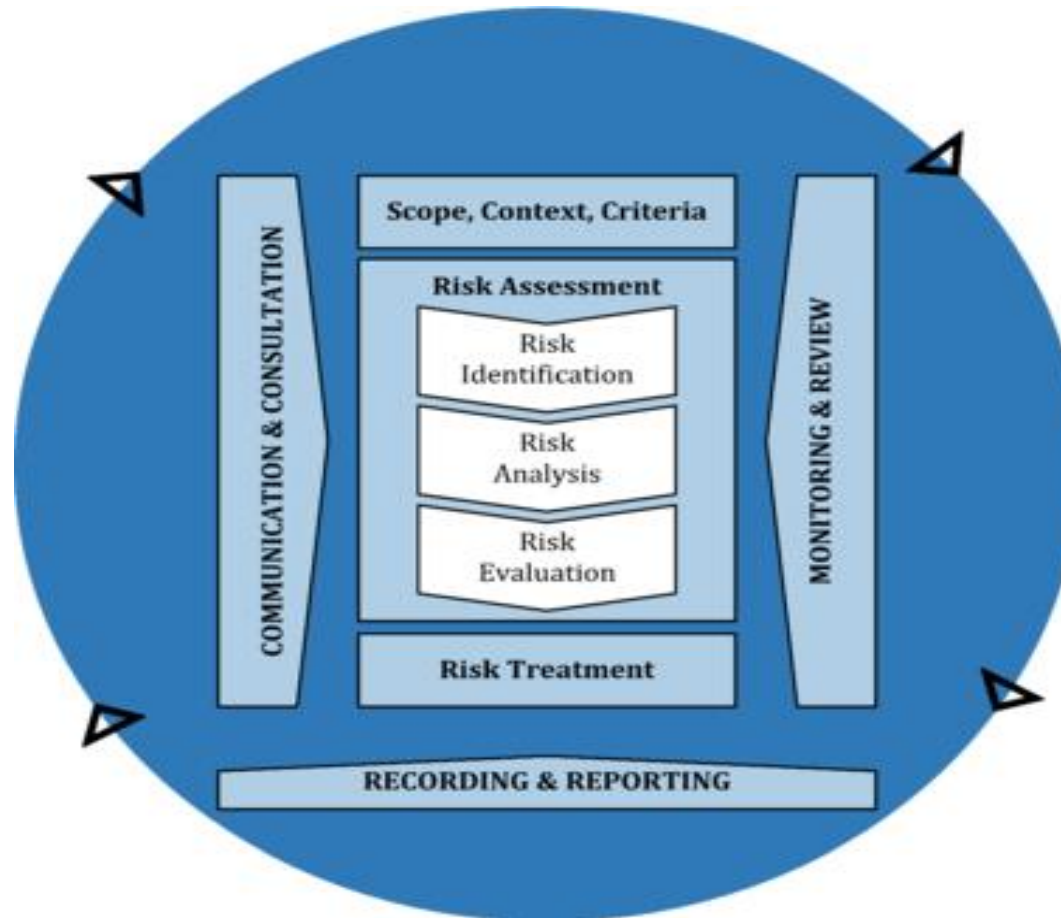
Framework



Lecture
04

ISO 31000:2018

Process



Where's the Value?

Lecture

04

ERM Frameworks

PMG 611

Enterprise Risk Management

Lecture

04

Where's the Value?

- Organizations are increasingly looking to expand their risk management functions to help reduce potential future losses through:
 - Improved monitoring and reporting
 - Better risk identification and response
 - More risk-based decision making
- The biggest value in each of these frameworks lay in their promotion of continuous improvement, diligent management practices and ongoing monitoring.

ERM is not...

- A silver bullet to prevent risks from occurring
- A methodology or a checklist of items that need to be completed that guaranteed results
- The only way organizations can take a more proactive approach to managing risk

Summary

Lecture

04

ERM Frameworks

PMG 611

Enterprise Risk Management

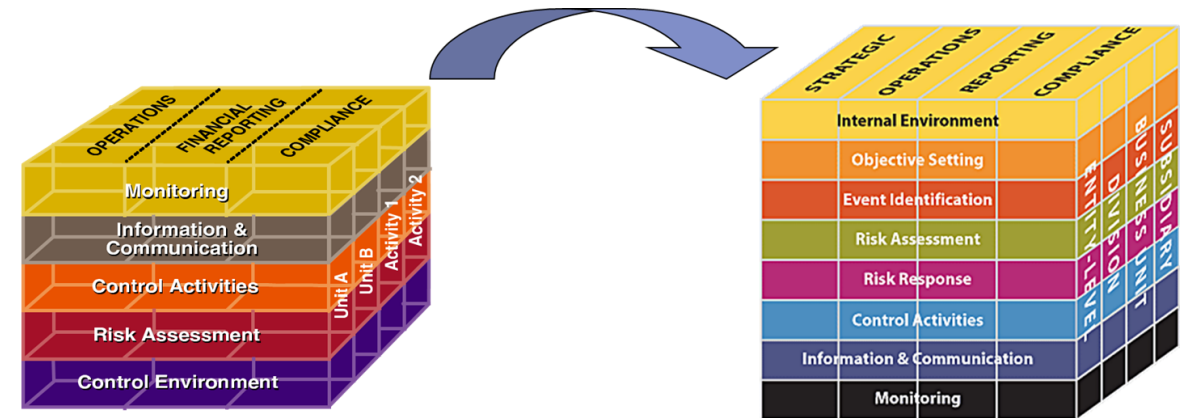


COMMITTEE OF SPONSORING
ORGANIZATIONS OF THE TREADWAY COMMISSION

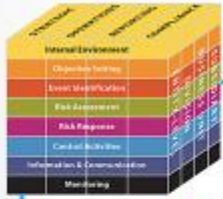
1. Enterprise Risk Management Integrated Framework (2004)
2. Enterprise Risk Management—Integrating with Strategy and Performance (2017)

COSO ERM Integrated Framework

To help assist with the implementation of the ERM process, COSO developed the ERM Integrated Framework (2004), also known as the *COSO Cube*. This cube is an update to the initial COSO I framework developed in 1992:



COSO ERM Integrating with Strategy and Performance



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

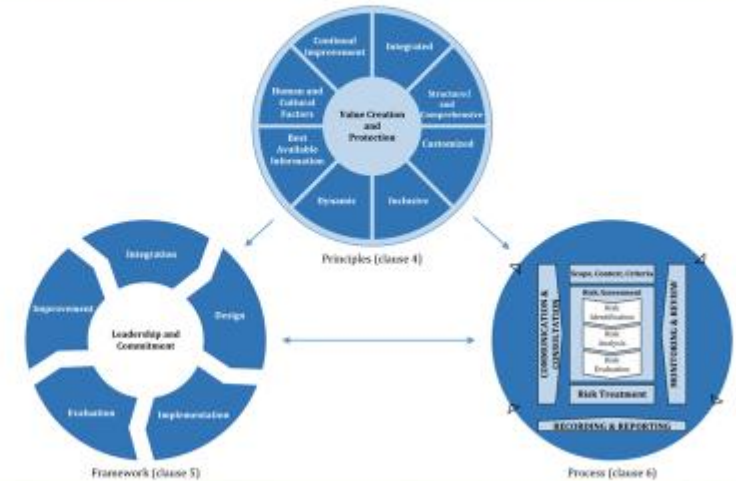
18. Leverages Information and Technology
19. Communicates Risk Information
20. Reports on Risk, Culture, and Performance

4-39

Lecture 04

ISO 31000:2018

<https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:en>



4-43

References

- COSO Enterprise Risk Management: Establishing Effective Governance, Risk, and Compliance Processes. *Robert R. Moeller*.
- 2017-COSO-ERM-Integrating-with-Strategy-and-Performance-Executive-Summary.
<https://www.coso.org/Pages/guidance.aspx>
- ISO 31000:2018(en) Risk management — Guidelines. <https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:en>



Thank You