Risk Management MN220:
Seminar 11
ERM Risk Management
- COSO Framework

SHERIDAN COLLEGE

PERTH | WESTERN AUSTRALIA

Seminar 11

Enterprise risk management (ERM)

- Enterprise Risk Management (ERM)
- Use of COSO framework

SHERIDAN COLLEGE
PERTH | WESTERN AUSTRALIA

Enterprise risk management[1]

"The process required to establish effective risk management as part of the day-to-day business at an organisational level and subsequently at operational, project or team levels is likely to require a change of culture for many organisations."[1]

[1]AS/NZS 4360:2004, Risk Management

ERM

- Term once frequently used to discuss the management of risk across the enterprise;
- Related to ”whole of business” rather than individual business process;
- Used less often today as risk management becomes more pervasive across and within the business.

BASIC EXTERNAL ANALYSIS

- PESTLE
- Using Coso

COSO framework explained

SHERIDAN COLLEGE
PERTH | WESTERN AUSTRALIA

- Link: https://www.youtube.com/watch?v=b7JldvsY7Ac&list=PL68AA245BF50F4A8C

Introduction

- In 1992, the Committee Of Sponsoring Organizations of the Treadway Commission (COSO) published Internal Control-Integrated Framework (1992 framework) which has become commonly known as the COSO framework.

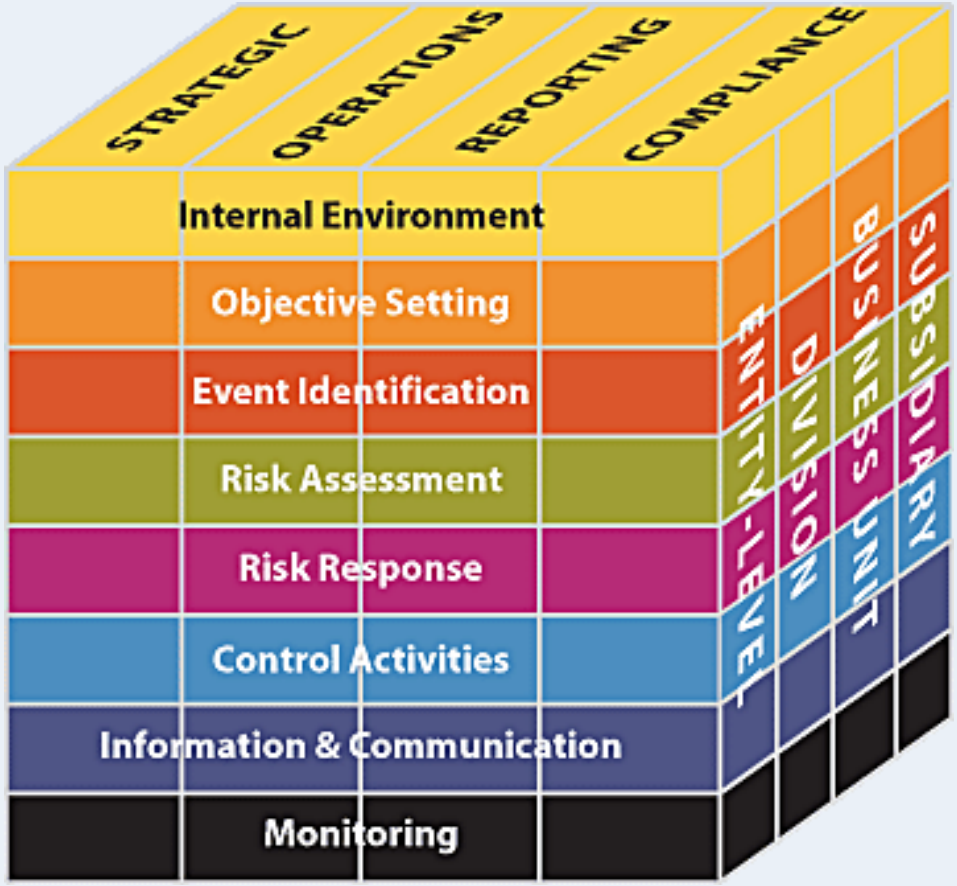
- In May 2013, COSO issued an updated Internal Control-Integrated framework (2013 framework) to reflect changes in the business world for over 20 years since the original framework.

1992 COSO Cube

2013 COSO Cube

SHERIDAN COLLEGE
PERTH | WESTERN AUSTRALIA

The COSO Cube Framework



SHERIDAN COLLEGE
PERTH | WESTERN AUSTRALIA

5 COMPONENTS OF THE COSO FRAMEWORK

17 PRINCIPLES OF THE COSO FRAMEWORK

Control Environment

1. Commitment to Integrity
2. Independence from Management
3. Establish Responsibilities
4. Commitment to Attract, Develop, and Retain Competent Individuals
5. Hold Individuals Accountable

Risk Assessment

6. Specify Objectives
7. Identify Risks
8. Consider Potential for Fraud
9. Identify and Assess Changes

Control Activities

10. Develop Control Activities to Mitigate Risks
11. Develop Control Activities to Support Achievement of Objectives
12. Deploy Control Activities through Policies

Information & Communication

13. Obtain Information to support internal control
14. Communicate Information
15. Communicate with external parties

Monitoring

16. Select, Develop, and Perform Evaluations
17. Evaluate and Communicate Internal Control Deficiencies

COSO COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION

2) Introduces Principles

20 key principles within each of the five components

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

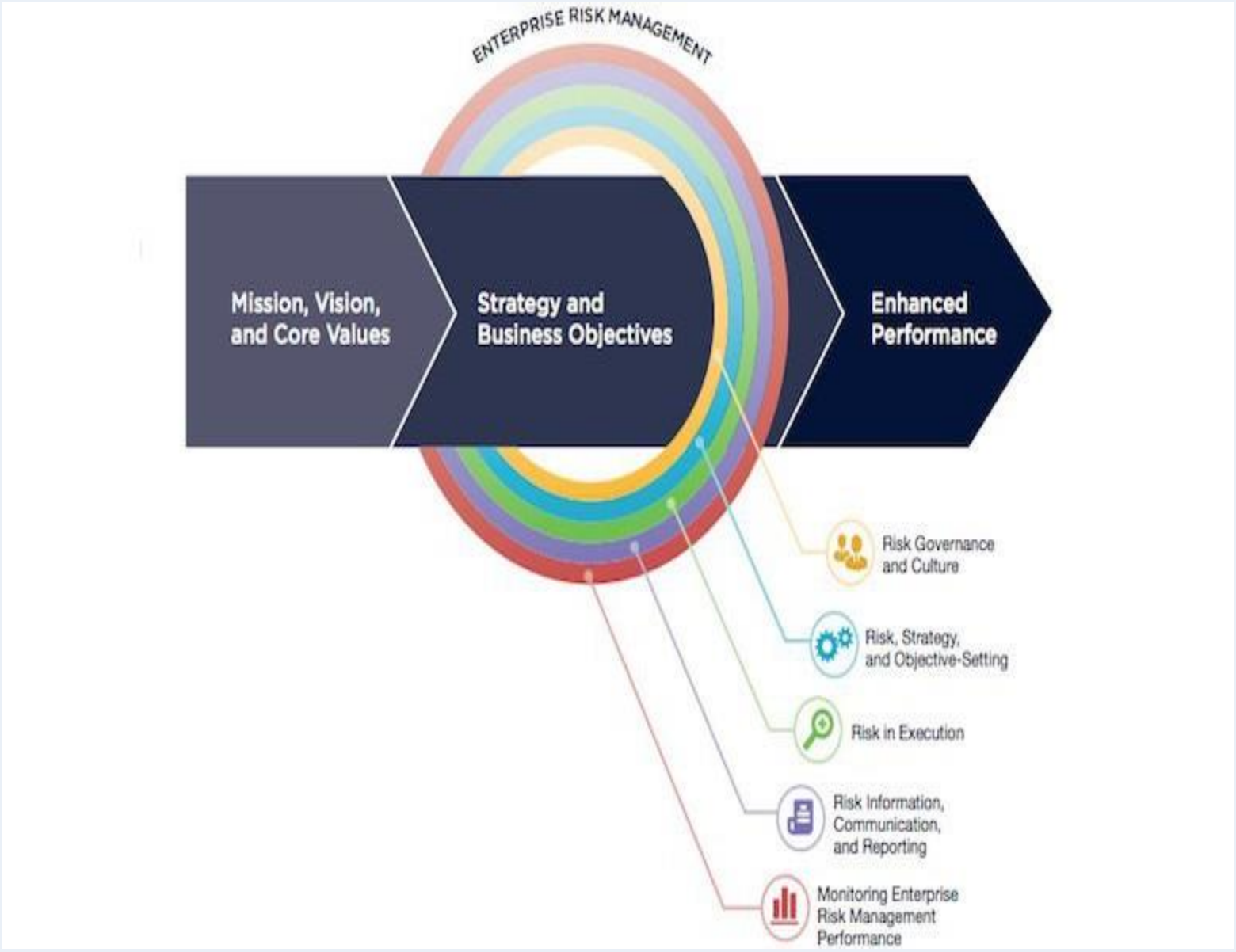
18. Leverages Information and Technology
19. Communicates Risk Information
20. Reports on Risk, Culture, and Performance

SHERIDAN COLLEGE
PERTH | WESTERN AUSTRALIA

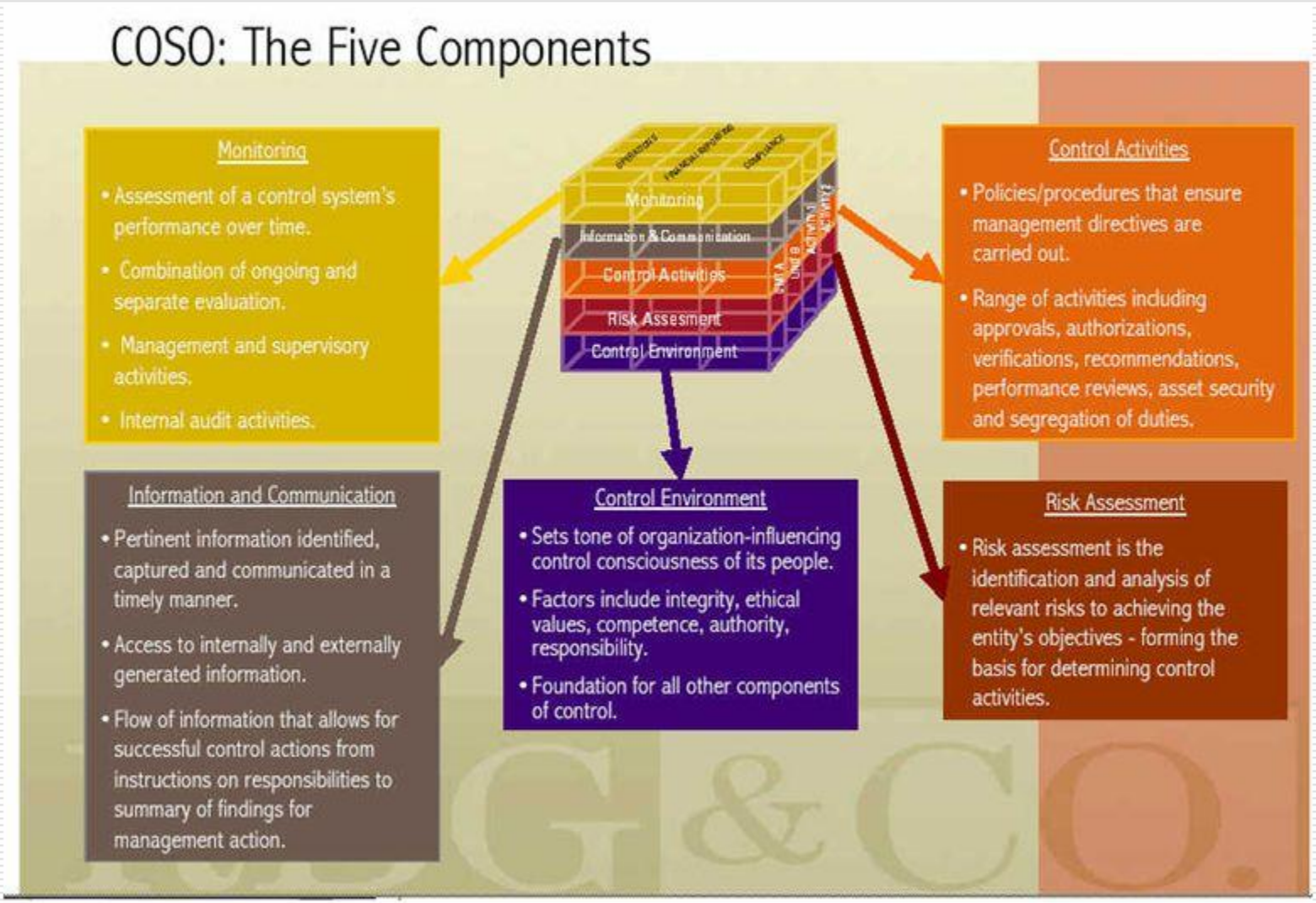
COSO COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION

6) Links to Strategy

- Explores strategy from three different perspectives:
  - The possibility of strategy and business objectives not aligning with mission, vision and values
  - The implications from the strategy chosen
  - Risk to executing the strategy


ENTERPRISE RISK MANAGEMENT
Mission, Vision, and Core Values
Strategy and Business Objectives
Enhanced Performance
Risk Governance and Culture
Risk, Strategy, and Objective-Setting
Risk in Execution
Risk Information, Communication, and Reporting
Monitoring Enterprise Risk Management Performance

COSO Control Framework



Widely Used ERM Frameworks

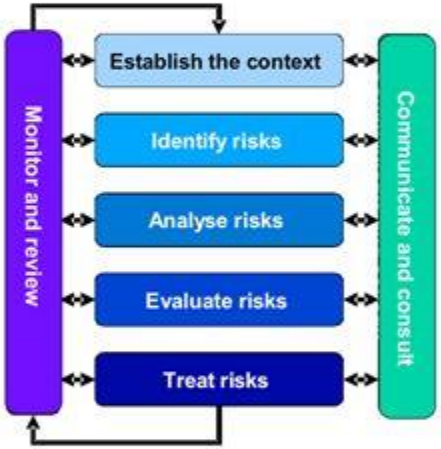
Similarities

Both frameworks require:

- Adoption of an enterprise approach, with executive level sponsorship and defined accountabilities
- Structured process steps, oversight and reporting of the identified risks
- Understanding and accountability for defining risk appetite and acceptable tolerance boundaries
- Formal documentation of risks in risk assessment activities
- Establishment and communication of risk management process goals and activities
- Monitored treatment plans

COSO vs. ISO 31000 Framework

Source: COSO



Source: ISO

Source: RIMS Executive Report – The Risk Perspective

SHERIDAN COLLEGE
PERTH | WESTERN AUSTRALIA

Summary

- Enterprise Risk Management (ERM);
- Establishing a risk management culture;
- Leadership, management and commitment;
- Interdependency between policy, goals, reward and sanction;
- Methodologies, processes, and outputs;
- Communication and consultation;
- Training and development;
- Integrating quantitative and qualitative elements of risk management.

SHERIDAN COLLEGE
PERTH | WESTERN AUSTRALIA

We trust you enjoyed participating in the journey of risk management. All the best for the exam!