

# **Risk Management**

## **MGM 510**

**Prepared by**  
**Dr. Hamed Almahadin**

**Lecture 6**



The background features a series of vertical panels with rounded ends. The first panel on the left shows a person's hands typing on a laptop. The second panel shows a graduation cap icon. The third panel shows a target icon, a play button icon, and a group of people icon. The fourth panel shows an open book icon and a magnifying glass icon. The fifth panel is a solid light blue color.

## **Ch#6**

# **Risk Management Standards**



Chapter  
**06**

## Topics to Cover in Week 6

- Risk management standards
- Scope of risk management standards
- IRM Standard
- COSO ERM Framework
- ISO 31000 Standard
- Risk management context

Chapter  
**06**

## Risk Management Standards

- There are a number of established risk management standards and frameworks.
- The first was developed by the standards body in Australia in 1995 and has been followed by those being developed in Canada, Japan, the UK and the United States.

Chapter  
**06**

## Risk Management Standards

- Standards have also been developed by other national standards bodies, as well as by government departments across the world.



Chapter  
**06**

## Scope of Risk Management Standards

- The international standard ISO 31000 (2009), 'Risk Management: Principles and Guidelines', was published in the latter part of 2009.
- Although some standards are better recognized than others, organizations should select the approach that is most
- relevant to their particular circumstances.

Chapter  
**06**

## Scope of Risk Management Standards

- It is important to distinguish between a risk management standard and a risk management framework.
- **A risk management standard** sets out the overall approach to the successful management of risk, including a description of the risk management process, together with the suggested framework that supports that process.

Chapter  
**06**

## Scope of Risk Management Standards

- In simple terms, a risk management standard is the combination of a description of the risk management process, together with the recommended framework.



## Chapter 06

# Scope of Risk Management Standards

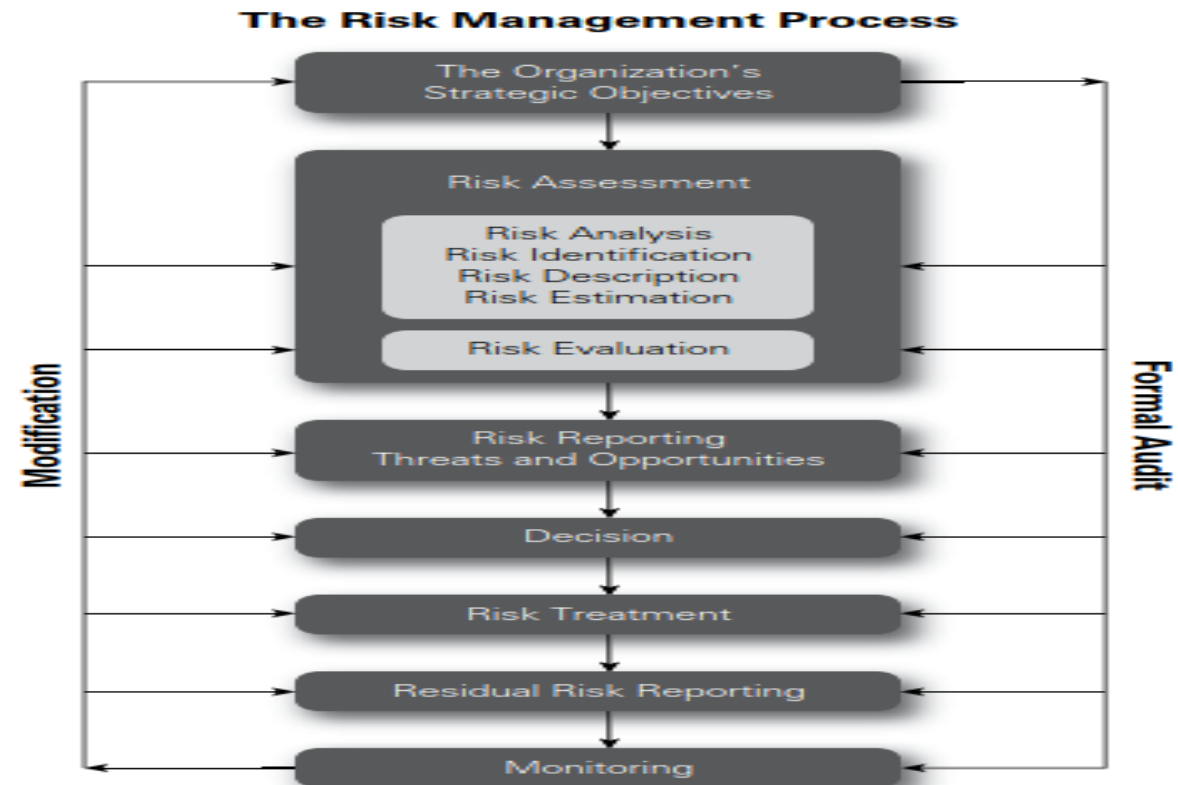
**TABLE 6.1** Risk management standards

| Standard                           | Description                                                                                      | Reference   |
|------------------------------------|--------------------------------------------------------------------------------------------------|-------------|
| ISO 31000                          | Standard published by the International Standards Organization (2009)                            | Figure 6.4  |
| Institute of Risk Management (IRM) | Standard produced jointly by Airmic, Alarm and the IRM (2002)                                    | Figure 6.1  |
| COSO ERM                           | Framework produced by the Committee of Sponsoring Organizations of the Treadway Committee (2004) | Figure 6.3  |
| CoCo (Criteria of Control)         | Framework produced by the Canadian Institute of Chartered Accountants (1995)                     | Figure 33.1 |

Chapter  
**06**

# IRM Risk Management Standard

**FIGURE 6.1** IRM risk management process





Chapter  
**06**

## IRM Risk Management Standard

- One of the best-established and most widely used risk management standards was produced by the IRM in 2002 in co-operation with Airmic and Alarm.
- The IRM Standard is a high-level approach aimed at non-risk-management specialists.



Chapter  
**06**

## Risk Management Process

- Although there are many ways of representing the risk management process, the basic steps are all similar.
- There can be difficulties with the terminology that is used to describe the various steps



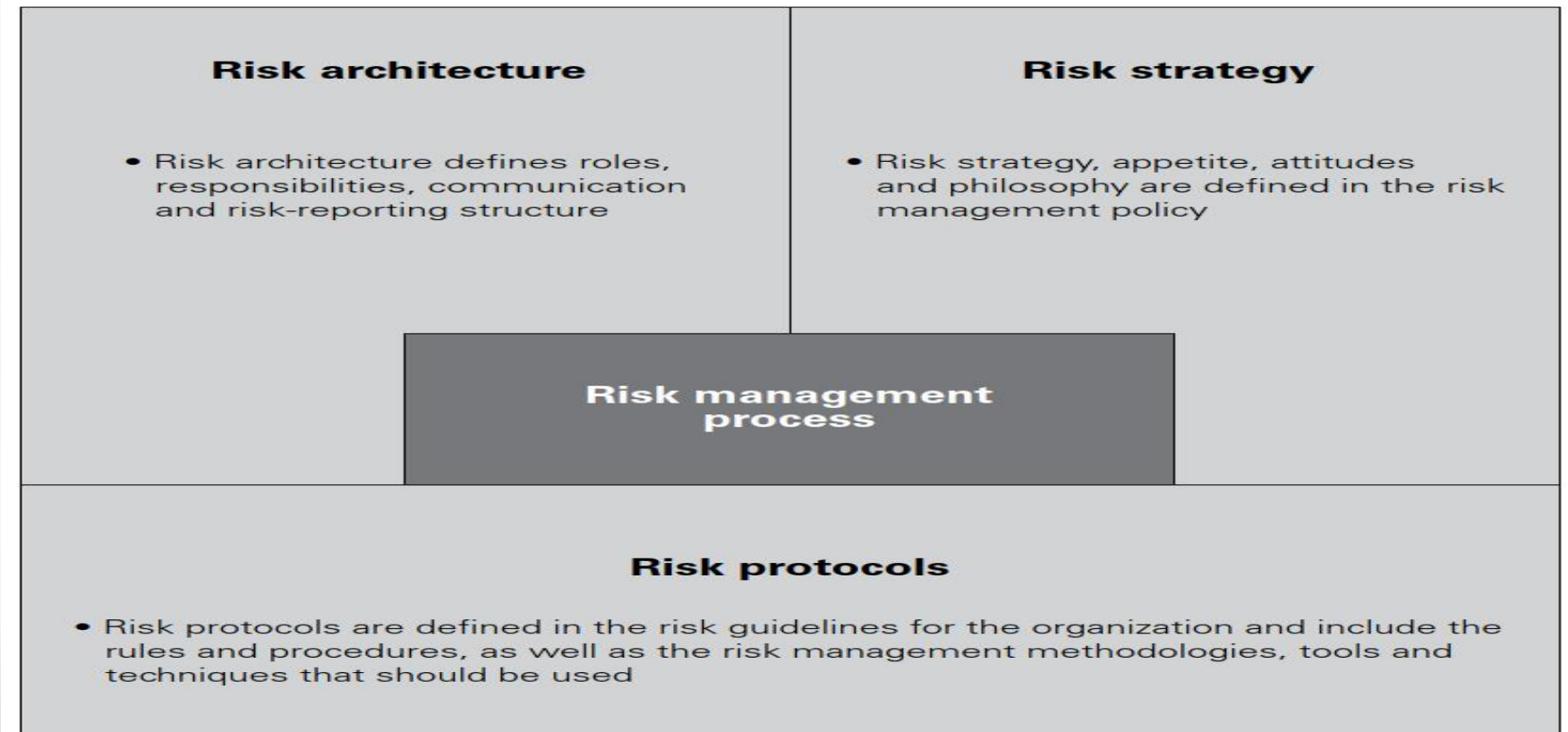
Chapter  
**06**

## Risk Management Context

- In order for the context to be described and defined, a framework is required to implement and support the risk management process.
- ISO 31000 places particular emphasis on context and states that consideration should be given to the internal context, external context and risk management context when undertaking risk management activities.

Chapter  
**06**

# Components of Risk Management Context





Chapter  
**06**

## Components of Risk Management Context

- These three components of risk architecture, strategy and protocols are required for successful risk management activities.
- There needs to be a clear understanding of the risk management process, followed by a clear definition of the framework that supports the process.



Chapter  
**06**

## Risk Management Framework

- In implementing and supporting the risk management process, the risk management framework needs to facilitate communication and the flow of risk information.
- The risk management framework has two separate considerations.

Chapter  
**06**

## Risk Management Framework

- Firstly, it must be supportive of the risk management process.
- Secondly, it must ensure that the outputs from the process are communicated into the organization and achieve the anticipated benefits for the organization.

Chapter  
**06**

## Risk Management Framework

- If an organization decides to follow the structure of the IRM Risk Management Standard, it would then have to set up a framework that includes the structure, responsibilities, administration, reporting and communication components of risk management.



Chapter  
**06**

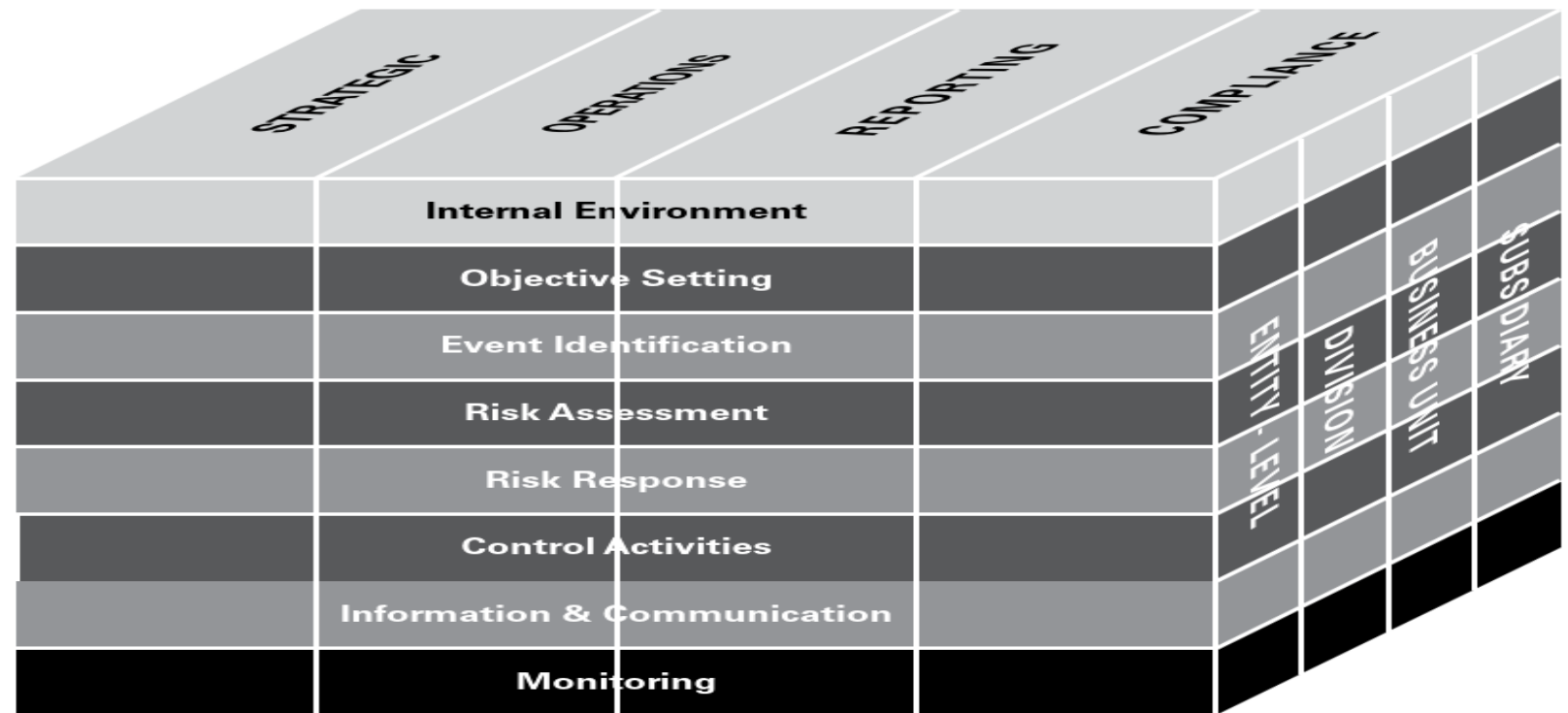
## COSO ERM Cube

- In the COSO ERM framework, there is a direct relationship between objectives, which are what an entity strives to achieve, and enterprise risk management components, which represent what is needed to achieve them.
- The relationship is depicted in a three-dimensional matrix, in the form of a cube, and this is reproduced as Figure 6.3.

Chapter  
**06**

# COSO ERM Cube

**FIGURE 6.3** COSO ERM framework



Chapter  
**06**

## COSO ERM Cube

- The COSO ERM cube is a very influential risk management framework and it consists of eight interrelated components.
- These are derived from the way management runs an enterprise and are integrated with the management process.
- A brief description of the COSO ERM components is set out in Table 6.2.

Chapter  
**06**

# COSO ERM Cube

**TABLE 6.2** COSO ERM framework

- Internal environment* – The internal environment encompasses the tone of an organization and sets the basis for how risk is viewed and addressed.
- Objective setting* – Objectives must exist before management can identify potential events affecting their achievement.
- Event identification* – Internal and external events affecting achievement of objectives must be identified, distinguishing between risks and opportunities.
- Risk assessment* – Risks are analysed, considering likelihood and impact, as a basis for determining how they should be managed.
- Risk response* – Management selects risk responses: avoiding, accepting, reducing, or sharing risk.
- Control activities* – Policies and procedures are established and implemented to help ensure the risk responses are effectively carried out.
- Information and communication* – Relevant information is identified, captured, and communicated so that people can fulfil their responsibilities.
- Monitoring* – The entirety of enterprise risk management is monitored and modifications made as necessary.

Chapter  
06

## COSO ERM Cube

This enterprise risk management framework is geared to achieving corporate objectives, set out in four risk categories:

- **Strategic:** high-level goals, aligned with and supporting its mission;
- **Operations:** effective and efficient use of its resources
- **Reporting:** reliability of reporting;
- **Compliance:** compliance with applicable laws and regulations.

Chapter  
**06**

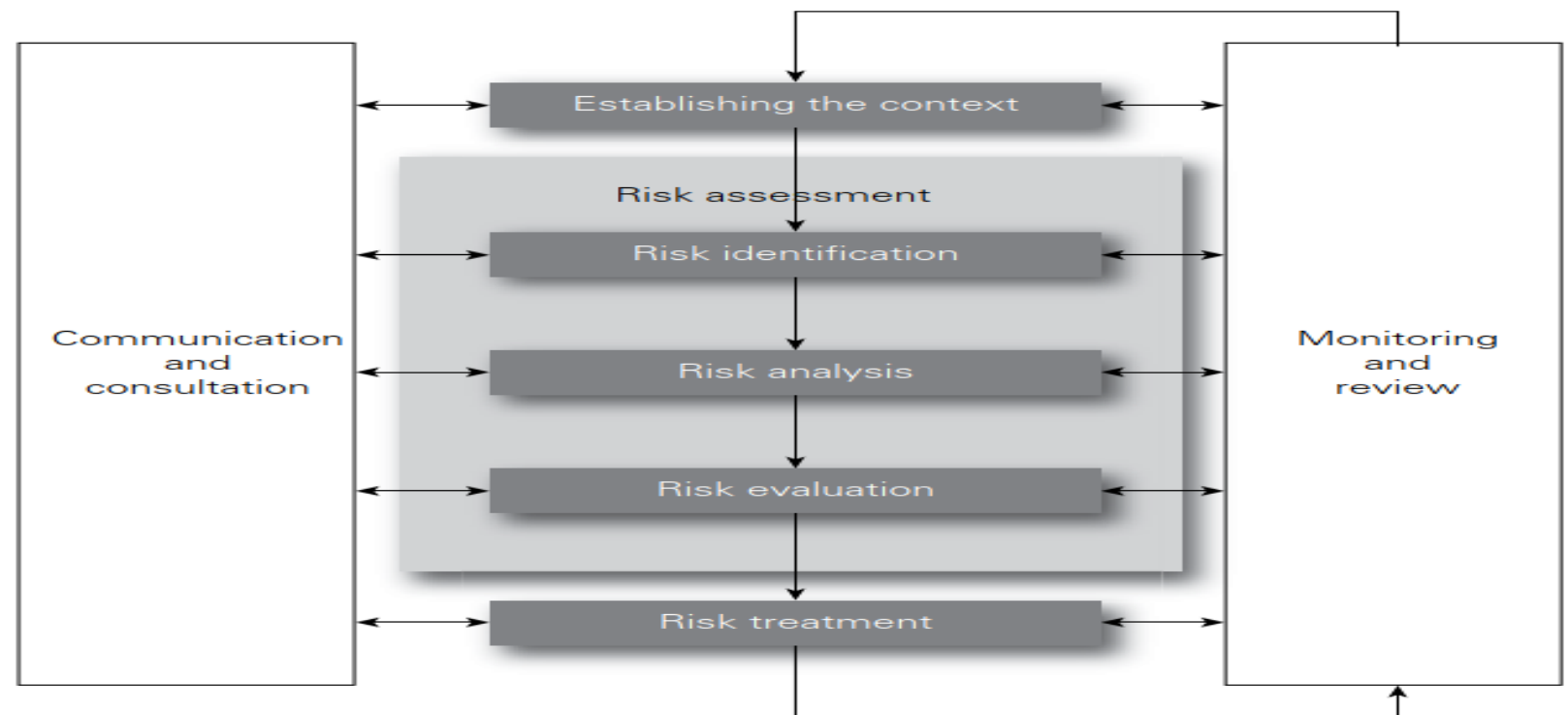
## COSO ERM Cube

- The International Standards Organization (ISO) published ISO 31000 entitled 'Risk Management: Principles and Guidelines' in the latter part of 2009.
- The diagram used to illustrate the risk management process in ISO 31000 is reproduced in Figure 6.4.

Chapter  
**06**

ISO 31000

**FIGURE 6.4** Risk management process from ISO 31000



Chapter  
**06**

## Risk Management Standards Selecting

- The challenge for standards organizations is to ensure that the risk management standards they publish are relevant to the future success of the organization.
- COSO has taken the approach, in updating the COSO ERM framework, that greater consideration should be paid to stakeholder expectations and the relationship between risk and strategy.

Chapter

## 06

## COSO

In particular, the COSO consultation document suggests that organizations that integrate enterprise risk management into strategic planning can obtain a range of benefits including:



Chapter  
**06**

**COSO**

- Increasing range of opportunities by considering both positive and negative aspects of risk;
- Improving performance by identifying and managing risk on an entity-wide basis;

Chapter  
**06**

**COSO**

- Reducing negative surprises, increasing gain and profiting from advantageous developments;
- Reducing performance variability by taking actions to minimize disruption;
- Improving resource deployment and achieving enhanced resource allocation.



Chapter  
**06**

## Scope of the Context

- The three components of context may be considered as follows:
- Risk management context has already been described as the risk architecture, strategy and protocols or the risk management framework within the organization.

Chapter  
**06**

## Scope of the Context

- This framework must fulfil two functions:
- 1) Provide support for the risk management process within the organization; and
  - 2) Ensure that the outputs from the risk management process are communicated to internal and external stakeholders.



Chapter  
**06**

## Scope of the Context

- Internal context refers to the organization itself, the activities it undertakes, the range of skills and capabilities available within the organization, and how it is structured.
- Internal stakeholders and their expectations are part of the internal context.
- This may be considered to be the strengths and weaknesses within the organization.

Chapter  
**06**

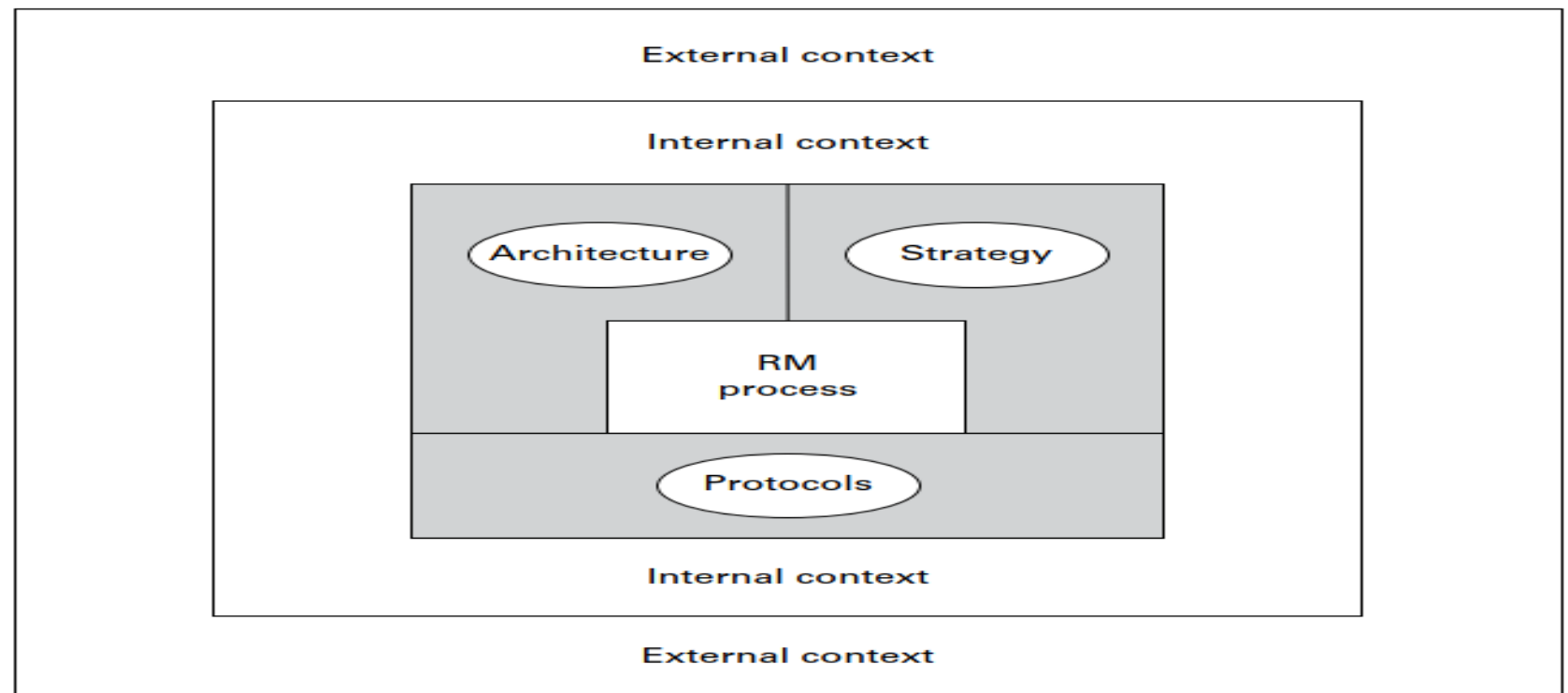
## Scope of the Context

- External context is the environment within which the organization exists.
- This environment will include consideration of the business sector within which the organization operates, external stakeholders and their expectations and the external financial environment.
- This may be considered to be the opportunities and threats facing the organization.

Chapter  
**06**

# Scope of the Context

**FIGURE 7.1** Three components of context



Chapter  
**06**

## Scope of the Context-External Context

- In summary, the reputational component of the external context for an organization defines the external perception of the organization and the desire of customers to trade with the organization and the level of customer retention

Chapter  
**06**

## Scope of the Context-External Context

In particular, when evaluating the reputational component of the external context, the following issues should be addressed:



Chapter  
**06**

## Scope of the Context-External Context

- Public perception of the industry sector in which the organization operates;
- Corporate social responsibility standards achieved by the organization;
- Governance standards and whether the sector is highly regulated;
- Quality of products or services and/or after-sales service standards.

Chapter  
**06****Scope of the Context-External Context**

In particular, when evaluating the marketplace component of the external environment, the following issues should be addressed:

- Level of revenue generation in the marketplace and return on investment;
- Presence of aggressive competitors and/or high customer expectations;

Chapter  
**06**

## Scope of the Context-External Context

- Level of economic stability, including exposure to interest rates and foreign exchange rates;
- Complexity of the supply chain and volatility of raw material costs;
- Exposure to international disruption because of political risks, war and terrorism.

Chapter  
**06**

## Scope of the Context-Internal Context

In summary, the financial component of the internal context of an organization defines the financial procedures and the means by which money is managed and profitability is achieved.

In particular, when evaluating the financial component of the internal context, the following issues should be addressed:



Chapter  
**06**

## Scope of the Context-Internal Context

- Availability of adequate funds to fulfil strategic plans;
- Existence of robust procedures for correct allocation of funds for investment;
- Nature of internal financial control environment to prevent fraud;
- Availability of funds to meet historical and anticipated future liabilities.

Chapter  
**06****Scope of the Context-Internal Context**

In particular, when evaluating the infrastructure component of the internal context, the following issues should be addressed:

- Senior management structure and the nature of the risk culture;
- Availability of adequate people resources and people skills, including intellectual property;
- Availability of adequate physical assets to support operational activities;



Chapter  
**06**

## Scope of the Context-Internal Context

- Information technology infrastructure sufficient to achieve resilience and protect data;
- Business continuity plans in place to ensure continuity of activities following major disruption;
- Arrangements for service delivery and/or transportation and reliable communication infrastructure.



مجموعة جامعة  
الجميع الذكية  
للتعليم القابضة

MIDOCEAN  
UNIVERSITY



# Thank You

