Course Learning Outcomes for Unit V

Upon completion of this unit, students should be able to:

5. Outline a risk management strategy, including a risk mitigation plan.
   5.1 Elaborate on the purpose, benefits, and challenges of establishing a business continuity plan (BCP), a disaster recovery plan (DRP), and a business impact analysis (BIA).

6. Assemble an organizational policy for planning and performing the risk management processes.
   6.1 Identify the purpose, benefits, and challenges of an operational risk management (ORM) strategy.

Course/Unit Learning Outcomes	Learning Activity
5.1	Chapter 12 reading Chapter 12 reading Unit lesson Unit V PowerPoint Presentation
6.1	Chapter 12 reading Unit lesson Unit V PowerPoint Presentation

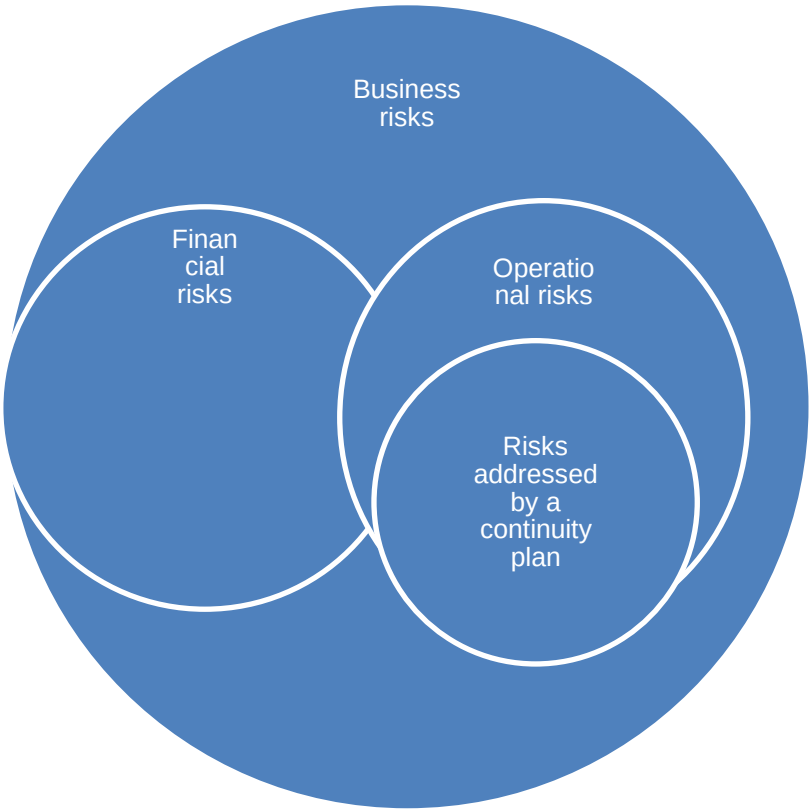
Reading Assignment

Chapter 12:
Operational and Logistical Security

Chapter 13:
Physical (Site) Security

Unit Lesson

Risk management applies to all aspects of an organization, across its operations, activities, and processes. As we have seen so far, risk management is useful in developing, applying, and employing an organization's total resources. Risk decisions should be based on awareness of the environment unique to each organization. Each organization is potentially exposed to a wide range of risks including financial, business, and operational risks. The graphic below depicts an organization's perceived risks.



Financial risks involve risk management across the entire organization including markets and liquidity of the enterprise. Business risks refer to the organization's compliance, economic performance, and any other factors affecting the business environment. Operational risks refer to threats from loss of resources including key personnel, theft, system failures, and building damage. Operational risk management aims to ensure and plan for the integrity and effectiveness of the organization. Operational risk management relies on various tools including audits, policies, system controls, and business continuity planning.

Operational Risk

Awareness of operational risk is low in many organizations, and very few of them have a sound business continuity plan (BCP) or disaster recovery plan (DRP) (Storkey, 2011). Few businesses have an *operational risk management* (ORM) strategy because it is not seen as important or inadequate resources are allocated to ORM, BCP/DRP efforts. In most organizations, ORM responsibility is delegated to information technology or becomes a one-off project rather than an essential part of the day-to-day organizational operations. Unfortunately, management's disregard for ORM strategies is frequently because of the belief that it will not happen to their organizations.

The challenge is that ORM covers a wide range of an organization's areas, often seen as covering all business aspects except the market, credit risks, and liquidity (Storkey, 2011). Operational risk is directly linked to business processes, procedures, systems in place, and effectiveness of management in every organization. Thus, operational risk is defined as the risk of loss as a result of the lack of or inadequate allocated resources, failed internal procedures, people, or systems.

ORM is seen as a competitive edge in most banks and financial institutions and is quickly being adopted in the non-financial sectors. There are two main drivers for ORM adoption: 1) a sound and effective operational risk management strategy facilitates the achievement of organizational objectives and performance, and 2) in many cases, operational risk management strategies help organizations meet regulatory compliance.

However, there are challenges in managing operational risks. As an example, developing a sound ORM strategy is complex, costly, and time-consuming. Implementing ORM systems requires resources and introduces complexities in existing business processes. In addition, implementing an effective ORM strategy requires buy-in at the top levels of management. Unfortunately, when it comes to ORM strategies, many

executives see ORM solely as a regulatory mandate and not as an enabler of competitiveness and business performance.

Business Continuity Planning (BCP) and Disaster Recovery Planning (DRP)

Business continuity planning (BCP) and disaster recovery planning (DRP) are elements of an operational risk management (ORM) strategy. Organizations implement a BCP to ensure uninterrupted availability of key business areas and resources that support business operations. The most important aspect of a BCP is that it helps organizations in preparing, preventing, managing, and recovering from events that are disruptive to the business. BCP addresses operational risks and assists in the planning and control of potential losses.

Organizations face many risks on a daily basis. There are many scenarios that could evolve into critical incidents potentially disrupting day-to-day business operations. Some of the scenarios could include the following disasters:

1. tornados;
2. flooding;
3. extended utility outages (electricity, water, gas);
4. hazardous materials release;
5. criminal activities;
6. disease outbreak;
7. civil unrest; and
8. mass casualty incidents.

A disaster recovery plan (DRP) refers to an organization's contingency planning focused on preventing disasters when possible and, in the event of a disaster, have a plan to avoid and minimize injury, minimize organizational loss, and manage recovery operations.

Thus, BCP and DRP improve the resilience of recovery and ensure that proper mitigation techniques are applied to organizational areas with unusually high or catastrophic exposure to risks. A BCP/DRP strategy helps in the avoidance or prevention of risk, identification of risk transference, risk containment, and risk acceptance or recovery.

Core Concept

The impact of threats to organizations can go beyond just financial losses; reputation and consumer confidence can also suffer.

Operational Security

Newsome (2014) defined operational security as the absence of risks in business operations. Operational security can be enhanced by minimizing the exposure of business processes and procedures to risks. A process by which an organization identifies and assesses risk is through a *business impact analysis* (BIA). A BIA is a key part of an organization's contingency planning process or DRP. A BIA includes a review of processes, procedures, assets, threats, vulnerabilities, and risks for the development of organizational strategic risk management. The product of the BIA is a report containing critical business elements detailing specific organizational areas and functions that could be affected should an unforeseen event or disaster take place.

A BIA assumes that every organizational unit depends on the continued operational functions of other units within the business. A BIA process will most likely uncover the priority of key business functions along with the sequence of recovery efforts from business unit to business unit. Whitman, Mattord, and Green (2014) articulated that one of the most critical aspects of a BIA is the analysis and prioritization of business processes as they relate to other business units within the organization.

Physical Security

Physical security, as defined by Newsome (2014), includes the physical approaches geared towards protecting personnel, safeguarding equipment, installations, and information against damage or loss. The damage or loss can come in the form of destruction, theft, or sabotage. The National Institute of Standards and Technology (NIST) handbook (2013) outlines specific critical areas where physical security is very important:

1. physical structures, assets, and elements (including information technology systems, storage facilities, and communication infrastructures);
2. the facility's geographical area, which could be susceptible to natural threats, man-made threats, or interception of transmissions; and
3. supporting facilities or structures (both technical and human) critical to the business operations.

CORE CONCEPT

Security access controls are processes wherein an organization's assets are made into a more difficult or less attractive target through physical, technical, and procedural mechanisms.

Summary

All organizations are subject to negative environmental events and unauthorized attempts to access their processes and structures. This may invalidate their use and cause potentially irreparable damage to all critical business units, including assets, individuals, and business procedures. An operational risk management framework with a BCP and DRP strategy ensures recovery and minimizes risk exposure through the implementation of a business impact analysis (BIA). A BIA assists in the identification, prioritization, and assessment of risks.

References

Newsome, B. (2014). *A practical introduction to security and risk management*. Thousand Oaks, CA: Sage.

Storkey, I. (2011). *Operational risk management and business continuity planning for modern state treasuries*. Retrieved from https://www.imf.org/external/pubs/ft/tnm/2011/tnm1105.pdf

Whitman, M. E., Mattord, H. J., & Green, A. (2014). *Principles of incident response and disaster recovery* (2nd ed.). Boston, MA: Course Technology, Cengage Learning.