Chapter VII
Information Systems
Risk Management:
An Audit and Control Approach

Aditya Ponnam
Louisiana State University, USA

Britta Harrison
Louisiana State University, USA

Ed Watson
Louisiana State University, USA

ABSTRACT
Organizations worldwide recognize the importance of a comprehensive, continuously evolving risk assessment process, built around a solid risk strategy that properly manages internal and external threats. A comprehensive enterprise risk management strategy must ideally contribute to the protection of the organizations’ assets, operations, shareholder’s value, and customer satisfaction while meeting imposed regulatory requirements and standards. As IT represents an integral part of the process required to achieve the aforementioned objectives, managing the risks associated with the information technology infrastructure of an organization is critical. The goal of this chapter is to review the most common risks and threat agents for a typical organizations’ information technology infrastructure and to discuss how systematic risk management procedures and controls can manage and minimize these risks.

INTRODUCTION
Defining and Understanding Risk and Control

Today’s business environment requires highly competent risk management functions with the capabilities to address a continuously changing risk profile.

In order to put risk in the proper context, two terms are defined (Stoneburner, Goguen, & Feringa, 2002): vulnerability, and threat. Vulnerability is a flaw or weakness in system security procedures, internal controls, or implementation that can be exercised (either accidentally or intentionally) and that can result in loss or harm. For example, a weak disaster recovery plan of an organization located in a disaster-prone area represents a vulnerability to the organization. A threat, such as a natural disaster, is the potential for a threat-source to exercise a specific vulnerability, such as a weak disaster recovery plan.
A risk is a circumstance or event that has the potential to hinder achievement of specific objective(s) or to cause harm. With respect to the previous example, the sudden disruption of a business or the loss of critical data in the event of a natural disaster is a risk that must be addressed. Therefore, organizations located in areas prone to environmental disasters should pursue a strong off-site data backup and recovery strategy by selecting a location less vulnerable to environmental disasters. A risk always has a cost associated with it. Once the vulnerabilities, threats, and respective costs are rated, risk can be interpreted by the following equation (Akin, 2002).

\[ \text{Risk} = \text{Threat} \times \text{Vulnerability} \times \text{Cost} \]

Cost is the total cost of the impact of a particular threat incurred by a vulnerable target. Costs are of three types: hard-dollar, semihard, and soft. Hard-dollar costs are measured in terms of “real” damages to hardware, software, or other assets, as well as quantifiable IT staff time and resources spent repairing these damages. Semihard costs might include such things as lost business or transaction time during a period of downtime. Soft costs include such things as diminished end-user productivity, damage to reputation, decreased stockholder confidence, or lost business opportunities (International Charter, 2006).

Business risks can be broadly classified into the following types (Business Link, 2006):

- Strategic (e.g., market competition, customer preferences, industry changes)
- Compliance (e.g., regulations, standards)
- Financial (e.g., foreign exchange, interest rates, credit)
- Operational (e.g., organizational culture, process risk, technology risk)
- Hazard (e.g., natural events, environment, physical employees)

These categories are not rigid, as some parts of your business may fall into more than one category. An environmental disaster threatening an organization’s ability to successfully back-up and recover data could, for example, potentially reach across and impact hazard, operational, financial, and compliance business risk categories.

Risks have the potential to deter an organization from achieving its goals and objectives. Management, therefore, must implement a risk control framework in order to prevent or mitigate risks to a level deemed acceptable to the organization.

It is important to understand the nature of controls. Controls are formal activities taken by business process owners to achieve an objective set by the organization to mitigate a respective risk. A control can be defined as a process, policy, or procedure designed to provide reasonable assurance that business objectives will be achieved. Controls, when exercised effectively, reduce or eliminate the exposure of a process to certain risks and, therefore, make the process less likely to incur losses associated with the risk. Controls can be preventive, detective, or corrective, as described below.

- **Preventive**: Implemented to prevent the risk from causing any loss or harm.
- **Detective**: Implemented in situations where it is important to understand that something adverse has happened. They warn of violations or attempted violations of organizational policy.
- **Corrective**: Implemented when the objective is to fix errant situations or events as they are identified.

Controls can be further classified as automated or manual (Rajamani, 2006).

- **Automated or programmed controls**: Automated controls are embedded within an organization's application systems and work in the background by virtue of the programming logic or application configuration, without any need for manual intervention. A financial application that calculates interest rates automatically based on a hard coded logic is an example of an automated control.
- **Manual controls**: These controls require a person to manually enforce the control. For example, a review and sign off that the quality of material obtained from a supplier has been inspected is a manual control.

**Information Technology and Risk: They Always Coexist**

In today’s globalized business environment, opportunities and risks go hand in hand. The more complex the business process and business model, the higher the scale and variety of risk that needs to be addressed. Risk also stems from poorly designed business processes, reliance on manual activities, use of legacy systems,