Chapter XXIV
Internal Auditing for Information Assurance

Sushma Mishra
Virginia Commonwealth University, USA

Amita Goyal Chin
Virginia Commonwealth University, USA

ABSTRACT

Internal auditing has become increasingly important in current business environments. In this era of the Sarbanes-Oxley Act and other similar legislations, regulatory compliance requires elaborate organizational planning. Auditing helps organizations in internal control assessment, change management, and better governance preparedness, thus enhancing information assurance. Various facets of internal auditing are discussed in this chapter and the role of internal auditing in information assurance is analyzed. Future issues and trends with internal auditing are also presented.

INTRODUCTION

Regulations including the Sarbanes-Oxley Act (SOX), the Health Insurance Portability and Accountability Act (HIPAA), the USA Patriot Act, and a plethora of others have created an urgency among business organizations for rapid compliance with governmental standards. Internal auditors play an increasingly important role in today’s business scenario, and therefore, have become in great demand. This is clearly evident from the recent surge in the job satisfaction and salary of internal auditors (Oxner & Oxner, 2006). Businesses often use internal auditors as in-house consultants, relying on them for adding value to a wide range of initiatives including management controls, financial reporting, information systems design, and fraud detection. Auditing plays an important role in securing information systems within organizations by including functions such as internal control assessment, controls over financial reporting, designing and implementation of information systems, vulnerability management, risk analysis, segregation of duties, adequacy of business controls, and the physical security of assets.

Recent developments in the regulatory environment have brought significant changes to the organizational outlook regarding internal auditing. Internal auditors are aware of these increased responsibilities and concentrate on discovering new ways of assuring the public about the integrity of organizational reports (Verschoor, 1991). Today’s business environment requires an audit process that supports the continuous assessment of the goals and objectives of information assurance. Organizational strategic goals must be tactically executed with performance measuring capability. For information assurance purposes, there should be close coordination between the audit team,
the security team, and the information technology operations (Bunker, 2003).

Information assurance (IA) can be viewed as an objective that involves all of the people, activities, and technologies employed to ensure that the fundamental properties of security—confidentiality, integrity, availability—are met throughout the lifecycle of a system (McEvilley, 2002). IA can be viewed as a process centric phenomenon that is comprehensive enough to include definition, implementation, and verification level operations. IA also includes day-to-day operations and the maintenance of the integrity of systems in such operational transactions. Assurance is subjective in nature and needs to be clearly explained to all involved in the security process.

Increasingly complex auditing functions require auditors to possess a deep knowledge about the organization and its business processes. Auditors should show an adequate understanding of the organizational culture, of the key players in the organization, and of the competitive environment in which the organization exists. Some audit practices that are becoming of heightened importance in today’s context include risk management and risk assessment. Recent research from the Institute of Internal Auditor’s Global Auditing Information Network (GAIN) indicates that given the various tools and techniques currently available to auditing teams, managing risks as well as consulting with management on aligning organizational goals within departments are considered extremely important. Audit functionality plays an important role in securing information systems in organizations by performing functions such as internal control assessment, risk analysis, segregation of duties, adequacy of business controls, and physical security of assets. Process and plan should have a clear statement of roles and responsibilities. An audit is also a means by which to ensure accountability from the management level of organizations. Accountability in management structures ensures better security management since governance objectives of securing informational assets can be reached in a systematic fashion. An accountability map provides security management programs with this critical component (Bunker, 2003).

This chapter explores the role of information technology (IT) auditing in the overall organizational information assurance functionality. Internal as well as independent audit functionalities are becoming a common practice for security purposes and there are various ways in which auditing can add value to an organization. The main objectives of this chapter are: to provide a background about audit functionality and discuss its expected functions; to provide an assessment of the importance of the role of auditing for information assurance purposes; to present the current audit practices for IT in general, and specifically, for information assurance purposes; and to discuss some future trends regarding the role of auditing in assurance.

BACKGROUND

The Institute of Internal Auditors (2006) defines the role of audit as:

*Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organization’s operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes* (p. 11)

Internal auditing has a broad focus, including individual transactions, control systems, and program operations. There are certain basic assumptions regarding the professionals in this field, necessitating that auditors retain the defining characteristics of credibility. To add value to an organization, auditors should be:

- Unbiased in their assessment. They are not just employees of a corporation but have a bigger societal responsibility.
- Systematic in their approach to collect and analyze information.
- Organized in using various criteria for formulating conclusions. Some of these criteria could include industry standards, goals/targets, benchmarks, and laws.
- Able to use widely accepted professional audit standards.

An organization has various stakeholders and public firms have an accountability towards their shareholders. Regulatory bindings require that the management of such public firms must periodically account to their investors for their use and stewardship of resources and to the extent to which the public’s objectives have been accomplished (The Institute of Internal Auditors, 2006). An effective audit activity