

# INFORMATION SECURITY GOVERNANCE AND INTERNAL AUDITS: A PROCESSUAL MODEL

**Sushma Mishra**  
Virginia Commonwealth University  
[mishras@vcu.edu](mailto:mishras@vcu.edu)

## Abstract

*Internal audits play an important role in risk mitigation, security governance, and information assurance in an organization. This research presents a processual model to conceptualize the audit function in an organization by addressing three fundamental questions about internal audits: what, why and how? The proposed model suggests that internal audits are an integral part of overall security governance and thus of an information assurance program in an organization.*

**Keywords:** internal audit, security governance, information assurance

## Introduction

Information security breaches are costly for organizations. Incidents such as Enron and Barings bank have totally changed the landscape of information security governance process. With the advent of the Sarbanes-Oxley act (commonly referred to as SOX), security governance has been redefined in terms of internal controls assessment and information assurance. Security governance can be viewed as structures and processes that ensure the integrity of the information flow and of business processes. Moulton and Cole (2003) conceptualize security governance as a way of establishing and maintaining a control environment to manage risks that relate to confidentiality, integrity and availability of information and its supporting processes and systems.

The Institute of Internal Auditors (2006) defines a systems audit as an “independent, objective assurance and consulting activity designed to add value and improve an organization’s operations”. Recent developments in the regulatory environment have brought significant changes to the organizational outlook regarding internal auditing. The strategic goals of organizations have to be tactically executed with performance measuring capability, across the enterprise. For information assurance purposes, there should be close coordination between audit teams, security teams and information technology operations (Bunker, 2003).

This paper argues that the systems audit function strengthens information security governance in an organization by adding value to an organization through information assurance. Systems audits have become an integral part of an organization’s information security governance process and the activities performed under audit help position an organization high in the eyes of investors. An efficient internal audit process of an organization provides assurance that the governance structures are strong and information systems are secure in an organization.

To understand the relationship between internal audit, security governance, and information assurance in an organization, this paper addresses the following questions:

- What do internal audits contribute towards security governance?
- How do internal audits add value to security governance?
- Why are internal audits important for security governance?

The intricate relationship between audits and security governance in an organization can be better understood by analyzing the process of interaction between audit functions and governance functions. By addressing the how, why and what of such an interaction, we will be able to assess the significance of internal audits in the overall governance process. A processual model showing this interaction is conceptualized. The rest of this paper is organized as follows: the next section presents an overview of relevant information security governance research. Section three presents a discussion on various aspects of internal audits and how it audits may add value in an organization. Section four describes the proposed model, capturing the impact of internal audits on information security governance. Section five reiterates the contributions of this paper, proposes future research directions, and points out some limitations.

## **Section 2: Information security governance**

The Certified Information Systems Auditor (CISA) review manual (ISACA, 2004) defines information security governance as a “focused activity with specific value drivers: integrity of information, continuity of services and protection of information assets”. Information systems security governance requires effective management of the technical aspects of security.

Ward and Smith (2002) emphasize the role of proper security policies as crucial for effective information systems security governance. A clear and concise security policy formulation is important for security governance (Campbell et al., 2002). Effective communication of these policies to employees enhances compliance of such policies (Lindup, 1996; Thomson and Solms, 2005; Karyadaa et al, 2005). Information security governance creates the blueprint for the organization’s plans to deal with security threats. A successful security governance effort will instill confidence by investors and the market in the organization and trust in announcements and reports by the organization. Management’s role in comprehensive information systems security governance is to appropriately delegate responsibility and accountability in organizational structures (Dhillon, 2001). Warkentin and Johnston (2006) argue that compliance with security governance procedures can only be achieved by enforcing internal controls. Periodic assessment of internal controls is important for operational efficiency, leading to less vulnerabilities and better security management (Flowerday and Solms, 2005; Rezmierski et al., 2002; Whitman, 2003).

## **Section 3: Internal audits and its benefits**

Today’s business environment exists within a plethora of legislation, and regulatory compliance has become a guiding factor in creating internal controls and other assurance measures. Internal auditing thus has an important role in an organization’s internal control assessment, compliance activities and assurance effort. An organization has multiple stakeholders, including the shareholders in the case of public firms. Regulatory bindings require that the management of such public firms must periodically give the investors an account of the use and stewardship of resources, and the extent to which the public’s objectives have been accomplished (The Institute of Internal Auditors, 2006). It is the ethical responsibility of auditors to provide the public an independent, objective evaluation of the accuracy of an organization’s accounting and risk mitigating plans, to provide assurance in the information provided by organization. The need for a third party to attest to the credibility of the financial reporting, performance results, compliance, and other measures arises from several factors inherent in the relationship between the investors and an organization (The Institute of Internal Auditors, 2006).

Organizations strive to develop an enterprise wide, completely integrated, audit and control model that can be used for improving audit results, corporate governance and regulatory compliance (Robitaille, 2004). Implementing an enterprise wide audit model leads to a high level of assurance, increased profitability, control documentation, and control training. Maintaining an audit issue database to house all outstanding audit issues is a good step towards ensuring better assurance (Robitaille, 2004). Each issue identified during the audit process should be registered, and corrective action should be taken against it. Even though many organizations dread auditing opportunities, in reality, assessments of auditors offer valuable benefits (Perkins, 2006). Auditor inputs provide IT staff and senior managers with a rare opportunity to step back from day-to-day concerns and re-evaluate direction, change strategy and enter new markets (Perkins, 2006). An effective audit team will provide good assessments that offer an impartial and comprehensive picture of IT concerns across the enterprise. Auditors must clearly describe the business demand for IT

services and the cost of those services, and they must provide an analysis of IT's capability to deliver. Such audit reports are important from a governance perspective.

## **Section 4: The proposed model**

In the conceptual model presented in figure 1 below, a processual view of the role of an audit in an organization's governance process is presented. The analysis of the process flow in the security governance environment is presented by looking at the *why*, *how* and *what* of the role of an internal audit in an organization. A description of the model is presented below:

### ***What***

This section analyzes the various objectives of an internal audit. What does an internal audit do for an organization or what is the end result of such an exercise? The internal audit primarily helps in the protection and assurance of informational assets in an organization. The audit is one way of providing management assurance about the major risks facing the organization (Roth, 2003). Accountability is added through all the process innovations and changes that have been prioritized, quantified, and linked to business results (Berk, 2006). Information security governance practices enhance information assurance through increased accountability and responsibility in an organization. The fundamental result of conducting an internal audit is to support the governance function in managing the informational assets.

### ***Why***

This section analyzes the plausible reasons for conducting an audit. Why internal auditing is required in an organization? One of the most important reasons to have internal audit, at least in today's regulatory environment, is for compliance purpose. Internal auditing has become mandatory to prepare for regulatory compliance with some of the complex regulations today such as SOX. From the compliance perspective, internal auditors typically assess the adequacy of corporate governance and the control environment in an organization; the effectiveness of the business processes to identify, assess, and manage risks; the assurance provided by control policies, procedures, and activities; the completeness and accuracy of information and communication systems and practices; and the effectiveness of management's monitoring and evaluation activities (The Institute of Internal Auditors, 2006).

Internal audit is also required to ensure business integrity in an organization. Auditors help in aligning organizational objectives with IT objectives. Internal audit departments have the daunting task of balancing controls and process efficiencies in a way that operational efficiency is not compromised (Berk, 2006). Auditors should have a process-improvement methodology and should assist process owners in conducting a value-added process review (Berk, 2006).

### ***How***

This section analyzes various ways in which internal audits help an organization. How does an internal audit facilitate governance measures? There are various ways in which auditing helps in assurance purposes:

#### **Internal control assessment**

Systems audits are designed to assess the full scope of the organization's financial and performance control systems and to identify deficiencies and recommend corrective actions (The Institute of Internal Auditors, 2006). Audits achieved through the implementation of proper IT controls mitigates IT risk and increases operational efficiency and effectiveness (Melancon, 2006).

#### **Process standardization**

Through process audits, a majority of the value driven activities by IT controls can be derived by implementing a small fraction of COBIT or any other controls-based framework (Melancon, 2006). Audits have the capability of creating a culture of change management which can transform low- and medium-

performing organizations into high performers, delivering more value to the business with less risk (Melancon, 2006).

### **Risk mitigation**

Internal auditors are not just internal watchdogs but play an important role in assurance and consulting activity. Audit departments offer a variety of other services such as (Roth, 2003): risk based audit (identifying risks in various business processes) and pre-implementation review (participating in systems development or reviewing development stages).

### **Training**

Auditors also add value through educating employees about the benefits of certain security measures in an organization (Roth, 2003). These involve self assessment (workshop administration, collecting data to address self controls) and internal control education (formal training program for awareness of internal auditors).

### **Outsourcing of IS controls and impact on outsiders**

The institute of internal auditors (IIA) and Information Systems Audit and control Association (ISACA) have established a common set of guidelines for risk assessment in case of outside vendors. Impact of outsourcing services outside the organization requires a tab on the vendors operations as well, since the vendor can provide a potential gateway for security breaches. Also an assessment on the impact of the outsider services on general IT and management controls needs to be reevaluated in this light.

The proposed conceptual model provides an understanding of the process of auditing, the intended reasons of establishing the audit function, and the plausible benefits of an effective internal audit team.

## **Section 5: Conclusion and future research**

Information assurance is achieved by enhancing security governance initiatives and adding value to business processes through an optimal balance of controls and efficiency. The suggested model presents a conceptual process oriented view of role of internal audit in information security governance by analyzing the why, how and what aspects of internal auditing. This research contributes to information security research theoretically by providing a theoretical model to understand the impact of internal audit. There is a lack of research in establishing the relationship between auditing and governance in IS research. There are certain limitations with this research. The model suggested is based on a conceptual analysis and published literature, but it has not been empirically validated. The list of benefits from the internal audit team is dependent on organizational resources to invest in auditing activities. Future research would involve validating the model in an organizational setting and studying the relationship between resources allocated for audit department and the intended benefits form such investments.

## **References**

1. Berk, J. (2006). Change Champions, *The Internal Auditor*; Apr, 63, 2, pp. 64-69
2. Campbell, R., Al-Muhtadi, J., Naldurg, P., Sampemane, G. and Mickunas, M. D. (2002). Towards Security and Privacy for Pervasive Computing. In Theories and Systems, Mext-NSF-JSPS International Symposium, ISSS 2002, Tokyo, Japan, 2002.
3. Dhillon, G. (2001). "Violation of Safeguards by Trusted Personnel and Understanding Related Information Security Concerns." *Computers & Security* 20(2): 165-172.
4. Flowerday, S and Solms, R. (2005). Real-time information integrity = system integrity+ data integrity +continuous assurances. *Computers & Security*. Vol. 24, pp. 604-613
5. Kanter, H., McEnroe, J. and Kyes, M. (1990). Developing and Installing an Audit Risk Model, *The Internal Auditor*, Dec, 47, 6, pp. 51-55
6. Karydaa, M., Kiountouzisa, E., Kokolakisb, S. (2005). Information systems security policies: a contextual perspective. *Computers & Security*. Vol. 24, pp. 246-260

7. Lindup, K. (1996). The Role of Information Security in Corporate Governance. *Computers & Security*, Vol. 15, pp. 477-485
8. Rezmierski, V.E., Seese, M.R and St. Clair II, N. (2002). University systems security logging: who is doing it and how far can they go? *Computers & Security*, Vol 21, No 6, pp 557-564, 2002
9. The Institute of Internal Auditors (IIA) (2006), The Role Of Auditing in Public Sector Governance, retrieved on 12/19/06 <http://www.theiia.org/index.cfm?bhcp=1>
10. Thomson, K. and Solms, R. (2005). Information security obedience: a definition. *Computers & Security*. Vol. 24, pp. 69-75
11. Melancon, D. (2006). Reaching Compliance Through Foundational IT Controls, *IT Audit*, Volume 9, December, retrieved on 12/19/06 <http://www.theiia.org/itaudit/index.cfm?catid=21&iid=509>
12. Moulton, R. and Coles, R.S. (2003). Applying information Security Governance, *Computers & Security*, 22, 7, pp. 580-584
13. Roth, J. (2003). How do internal auditors add value? *The Internal Auditor*, Feb, 60, 1, pp. 33-37
14. Ward, P. and Smith, C. (2002). The Development of Access Control Policies for Information Technology Systems. *Computers & Security*. Vol. 21, No. 4, pp. 356-371
15. Whitley, J. (2005). IIA Issues IS Audit Guidance, *The Internal Auditor*; Jun, 62, 3, pg. 24
16. Whitman, M. (2003). "Enemy at the Gate: Threats to Information Security." *Communications of the ACM* 46(8): 91-95.

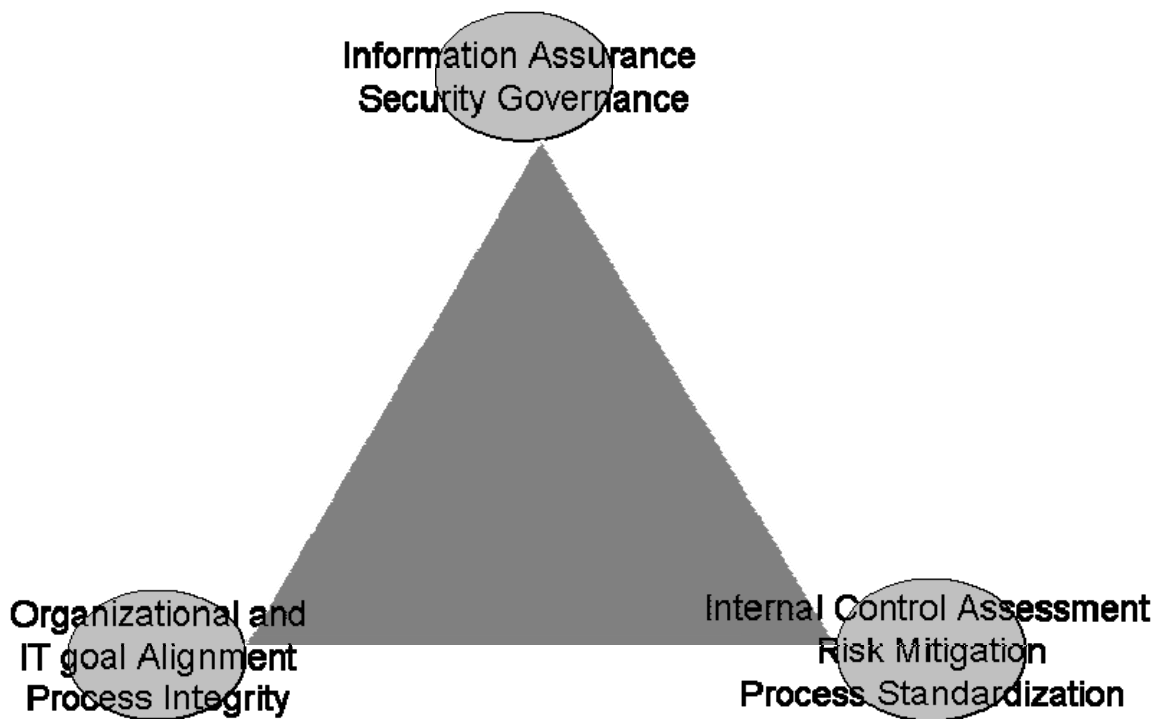


Figure 1: Processual model for role of internal audit in organization