Journal of Contemporary Management
Submitted on 07/01/2014
Article ID: 1929-0128-2014-02-22-07
Michael S. Lapke, and David L. Henderson III

Integrated Activities in Information Technology Auditing and Their Area Distribution

Dr. ***Michael S. Lapke*** (Corresponding author)
Assistant Professor of Management Information Systems
College of Business, University of Mary Washington
1301 College Avenue, Fredericksburg, VA. 22405, USA
Tel: +1-540-654-1713 E-mail: mlapke@umw.edu

Dr. ***David L. Henderson III***
Assistant Professor of Accounting
College of Business, University of Mary Washington
1301 College Avenue, Fredericksburg, VA. 22405, USA
Tel: +1-540-654-1918 E-mail: dhender3@umw.edu

***A*bstract:** Integration of business process and Information Technology audits is the optimal scenario when it comes to auditing. Despite this, audit departments are generally segregated and operate in 'silos' (KPMG, 2009). One of the first steps toward increasing adoption of the integrated approach is to benchmark current IT audit activities by identifying which IT audit activities are most frequently conducted in segregated audits and which IT audit activities are most frequently integrated into business process audits. Based on 1,457 survey responses from Chief Audit Executives, this paper identifies which IT audit activities are most frequently conducted in integrated audits and which IT audit activities are most frequently included in separate IT audits. The results showed that many internal audit organizations still use the segregated approach and that these organizations should further integrate change control audits into business process audits.

JEL Classifications: M40, M41, M42, M15

Keywords: Information Technology Auditing, Financial Auditing, Audit Integration

1. Introduction

As organizational Information Technology (IT) architecture has progressed, business processes have become increasingly integrated into the underlying IT infrastructure of the firm, resulting in an inseparable connection between business processes and IT (Ross, 2003; Venkatesh, 2006). As a reflection of the link between IT and business processes, a significant component of internal audit planning is determining the depth of assimilation of IT audit activities into business audit activities. IT audits can be conducted separately, on a stand-alone basis, or integrated into the business audit. In integrated audits, IT audit activities are conducted within business audits. IT audit activities are planned and executed under a multidisciplinary team possessing both business and IT audit knowledge. On the other hand, stand-alone IT audits are separated from business audits and have their own audit universe and scope.

Researchers and practitioners in the internal audit domain argue that, rather than conducting separate and isolated business and IT audits (referred to hereafter as the segregated approach), IT

audit and business audit activities should be integrated and executed as a single and integrated business/IT audit (referred to hereafter as the integrated approach) (Chaney & Kim, 2007; Rehage Hunt & Nikitin, 2008; Helpert & Lazarine, 2009). Integrated audits are characterized by a high degree of collaboration and interactivity between business auditors and IT auditors. Since the integrated approach simultaneously considers business processes and IT, as well as the interdependency between manual and technology-based controls, it is more likely to identify the impact of technological risks on business processes (Chaney & Kim, 2007; Helpert & Lazarine, 2009; Brand & Sagett 2011). In addition, the integrated approach offers the possibility to increase audit efficiency. This is due to the fact that audits of IT-driven processes can be conducted together with fewer auditors (Chaney & Kim, 2007; Helpert & Lazarine, 2009; Brand & Sagett 2011).

Despite the benefits of the integrated approach, the segregated approach remains the more popular approach (KPMG 2009). One of the first steps toward increasing adoption of the integrated approach is to benchmark current IT audit activities by identifying which IT audit activities are most frequently conducted in segregated audits and which IT audit activities are most frequently integrated into business process audits. Based on 1,457 responses from Chief Audit Executives to survey data acquired from the Institute of Internal Auditors' (IIA) Global Audit Information Network (GAIN) Annual Benchmarking Study (ABS) database, this paper identifies which IT audit activities are most frequently conducted in integrated audits and which IT audit activities are most frequently included in separate IT audits. The results of this study hold important implications for internal audit managers who are interested in implementing the integrated approach. By illustrating which IT audit activities are most frequently included in separate IT audits, the results of this study will help Chief Audit Executives to benchmark IT audit activities in their own internal audit departments.

2. Overview of Integrated Approach

Internal audit managers usually choose between three integration scenarios: low integration, partial integration, and high integration (Rehage, Hunt & Nikitin, 2008). The first of these, the low integration approach, dictate that IT audits are isolated and have their own audit universe and scope. Reviewing IT general and application controls are conducted and planned by a dedicated IT audit team and are activities that are conducted during an IT audit. The partially integrated approach has IT auditors and business auditors work together and jointly conduct application reviews. The highly integrated approach sees IT audit activities that are conducted within business audits. IT audit activities are planned and executed under a multidisciplinary team possessing both business and IT audit knowledge. Integrated audits are set apart from the prior two audits by a high degree of collaboration and interactivity between business auditors and IT auditors.

Audits focus simultaneously on an organization's financial, operational, and IT controls and processes under the integrated approach, ''Integrated audits not only save time and money, they also address true business risks in thoroughly integrated findings'' and are more ''likely to identify points of exposure" (Helpert and Lazarine, 2009). The integrated approach generates a comprehensive audit plan in which IT risks are assessed along with audits of the supported business areas (Marks & Taylor, 2009). As a result, the integrated approach results in more efficient and effective audits. This is especially important during a time of lower budgets (Pricewaterhouse Coopers, 2009). By addressing IT and business risks at the same time, integrated audits allow internal audit departments to more holistically consider and evaluate risk and focus audit efforts on high impact areas, thereby enabling a better understanding of the overall system of controls supporting key business processes (Brand & Sagett 2011).

Although the integrated approach may represent the optimal scenario all too often, audit departments are segregated and operate in 'silos' (KPMG, 2009). Segregated audits are not one thoroughly integrated audit, but rather two separate reviews: a business audit of the organization's financial and operational control processes and another of the organization's IT controls and processes (Chaney & Kim, 2007; Helpert & Lazarine, 2009). In the segregated approach, business auditors and IT auditors usually conduct their own risk assessments and then subsequently staff and perform the audit separately (Brand & Sagett, 2011). Business auditors and IT auditors use their own protocols and standards for communication. They also produce their own separate audit documentation (Brand & Sagett, 2011). The resulting audit documentation is then delivered to different stakeholders. The business auditor report is typically delivered to the manager of the business process (e.g., payroll manager) and the IT auditor report is delivered to IT leadership (Brand & Sagett, 2011). As a result, audit results may not be shared across business/technology clients (Brand & Sagett, 2011).

Since, in the typical segregated scenario, IT audit activities and business audit activities are conducted separately, segregated audits fail to account for the relationship between manual and automated controls and may result in the appearance of a disconnected audit team as well as different assertions over the same control (Chaney & Kim, 2007; Helpert & Lazarine, 2009). The lack of integration between the IT auditors and business auditors is not likely to produce a cohesive account of risk and control deficiencies. Instead of collaboratively evaluating the business risks and providing a holistic perspective on risk, IT auditors and business auditors produce their own discrete findings and then combine audit findings in a fragmented manner during the reporting phase. Furthermore, since the audit reports go to different managers, the segregated approach may result in missed opportunities to uncover risks that may have a significant impact when considered holistically (Brand & Sagett, 2011).

3. Data Collection and Analysis

The data used in this study to identify which IT audit activities are most frequently conducted in integrated versus segregated audits were collected by the IIA through their GAIN ABS (https: //na.theiia.org/services/gain/pages/gain-benchmarking.aspx) survey for the years 2007 through 2009. The GAIN ABS database consists of Chief Audit Executives' (CAE) responses to a comprehensive survey which is designed to measure various aspects of an organization's internal audit activities. The annual survey gets information regarding several IT-related topics including IT-related training approaches, possession of IT knowledge, and depth of IT-business audit integration. The GAIN ABS covers a broad range of institutions including publicly traded companies, private companies, educational institutions, and governmental institutions. The survey includes participants from 16 industries, over 100 sub-industries, and over 40 countries.

The data were analyzed via frequency distributions to determine how frequently each IT audit activity (e.g., assessing logical access controls) is conducted as part of an integrated audit or distinct IT audit. A summary of the entire set of data can be seen in Figure 1 on the next page.

3.1 Most Integrated Areas

As shown in Figure 2 on the next page, the most integrated areas include access control, business applications, physical security, and end user computing. Of these areas, only access control and business applications are more than 50% integrated. Areas in which the amount of integration has significantly increased from 2007 to 2009 include: Major Integration, Existing Business Applications, Information Management, End User Computing, Improvement IT Systems, E-Commerce, Strategic Plans, New IT Applications, Application Change Control, and Access Controls.

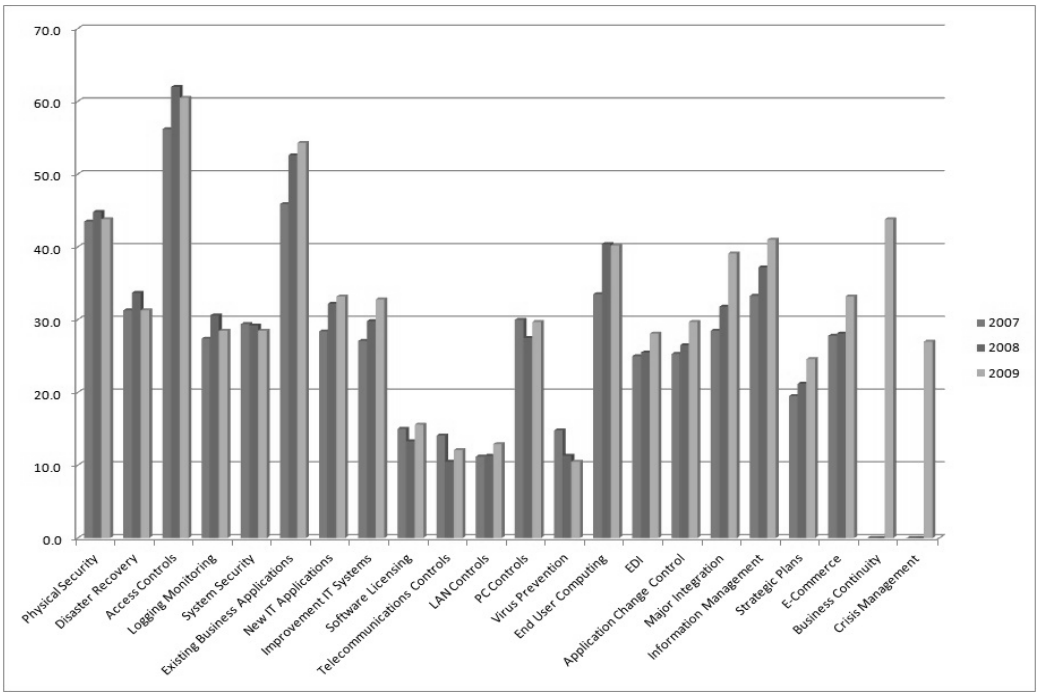

Figure 1. Integration for all areas

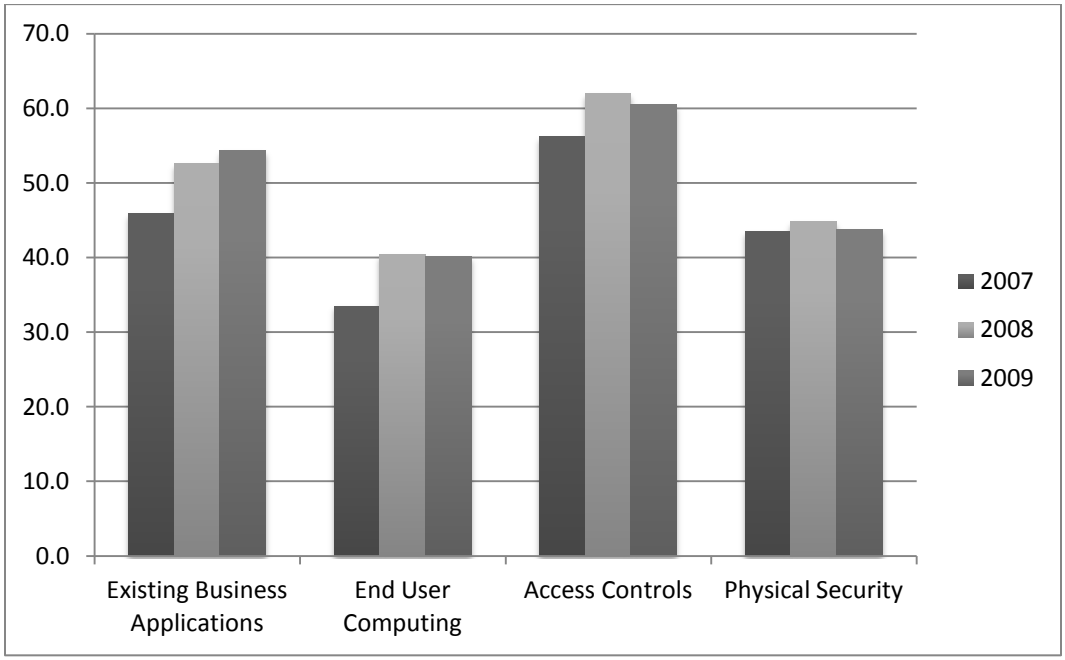

Figure 2. Most integrated areas

Figure 3 below highlights the areas with a relatively significant increase in integration between 2007 and 2009.

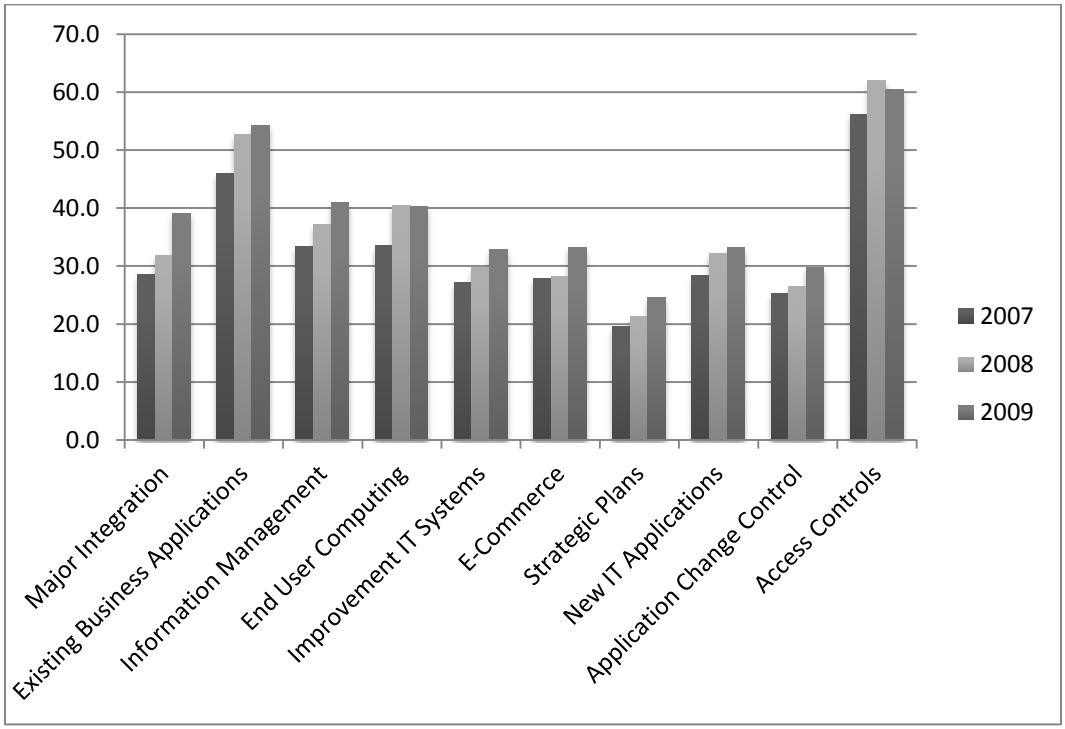

Figure 3. Areas with relatively significant increases in Integration

The finding that the access control and business application control areas are the most integrated areas is not surprising. The business applications control area refers to application controls. When reviewing application controls, especially in an Enterprise Resource Planning software environment, internal auditors should use the business process method. This would take the form of the Global Technology Audit Guide (GTAG 8), Application controls. Internal auditors need to include within the review's scope the separate applications that make up the different components of the business process cycle. The auditor can then identify the inbound and outbound interfaces within the application under review and complete the scoping activity. The internal auditor needs to have a thorough understanding of the modules that comprise the business process and how the data is managed and flows from one module to the other.

The importance of the access control and business application control areas is reflected in Auditing Standard 5 (AS5) distributed by the Public Company Accounting Oversight Board (PCABOB). This recommends a top-down approach to controls testing that focuses on those internal controls most relevant to the risk of material misstatement (Jabulani, 2007). As a result, internal auditors may focus on application controls, which have a strong relationship with the risk of material misstatement (Jabulani, 2007). Similarly, weak access controls can also result in a high risk of fraud or material misstatement. As such, it is not surprising that access controls are the most integrated area.

Another control area that should be highly integrated into business process audits is change controls. Change controls are important because changes made to a system that supports the financial reporting process can impact compliance with Sarbanes-Oxley. Uncontrolled changes in

production can lead to errors that, if pervasive or critical, could be considered significant deficiencies. Where key financial controls are impacted or the organization has failed to correct significant IT general control deficiencies identified in the prior year (such as in change management), management may face the possibility of having to deal with material weaknesses. Despite the importance of change controls, our findings indicate that they are not typically addressed in integrated audits, but rather in stand-alone audits. Given the benefits of the integrated approach and the importance of adequate change controls for maintaining SOX compliance, internal audit managers should assess change controls in conjunction with business audits, rather than as stand-alone IT audits. Although our findings suggest that change controls are not frequently assessed in integrated audits, their degree of integration is increasing.

3.2 Least Integrated Areas

On the other hand, the least integrated areas include software licensing, telecommunications controls, local area network (LAN) controls, and virus prevention. These areas are illustrated in Figure 4. Further from 2007 to 2009, virus prevention is the only area showing a consistent downward trend in integration. This downward trend can be seen in Figure 4 as well.

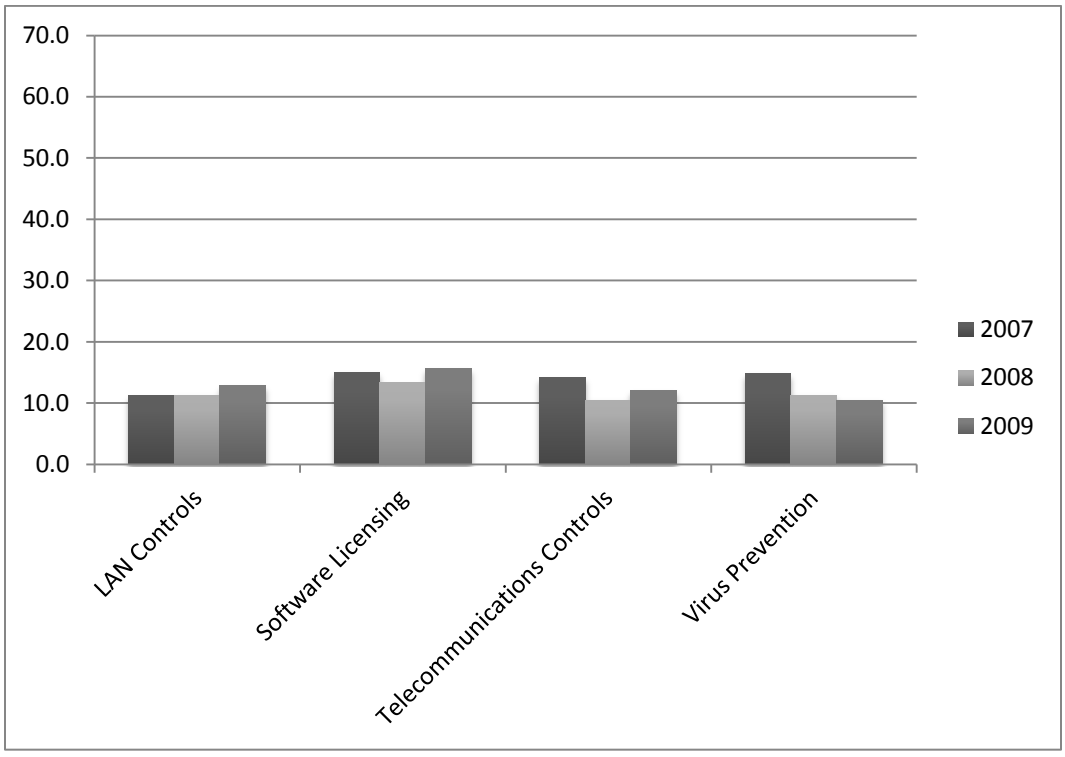

Figure 4. Least integrated areas

Software licensing, telecommunications controls, LAN controls and virus prevention are IT general controls. One potential reason for why these controls are not highly integrated is that since IT general controls have an indirect relationship with the risk of material misstatement, business auditors may spend less auditing IT general controls under AS5 and more time testing application controls (Jabulani, 2007).

4. Conclusion

Although internal audit experts have strongly advocated the integrated approach, many internal audit organizations still use the segregated approach (KPMG, 2009). This paper illustrates those internal control areas that are most integrated and those control areas that are least integrated. Internal audit managers can use the results of this study to benchmark their own control areas and identify areas for improvement.

Our results indicate that a sizable portion of the areas of study show an increase in integration over the two year span. Furthermore, only one control area has showed a consistent downward trend, suggesting that internal audit managers are beginning to see the benefits of the integrated approach. Further education and outreach efforts should be conducted to advertise the benefits of the integrated approach and encourage its adoption.

References

[1] Bellino and Hunt (2007), "Global technology Audit Guide: Auditing Application Controls", Altamonte Springs, FL: Institute of Internal Auditors.

[2] Brand, D., & Sagett, A. (2011), "Integrated Auditing for a Small Department", Retrieved from: http://protiviti.com/en-US/Pages/Integrated-Auditing-for-a-Small-Department.aspx

[3] Chaney, C. & Kim, G. (2007), "The Integrated Auditor", *Internal Auditor*, 64(4): 46-51.

[4] Helpert, A., & Lazarine, J. (2009), "Making Integrated Audits Reality", *Internal Auditor*, 66(2): 37-40.

[5] Jabulani, L. (2007), "Auditing Computer Controls with AS5", Retrieved from http://www.complianceweek.com/pages/login.aspx?returl=/auditing-computer-controls-with-as5/article/185267/&pagetypeid=28&articleid=185267&accesslevel=2&expireddays=0&accessAndPrice=0

[6] KPMG (2009), "IT Internal Audit Survey", Retrieved from: http://www.isaca-malta.org/live/attachments/219_KPMG%202009%20IT%20internal%20audit%20survey.pdf

[7] Marks, N., & Taylor, J.R. (2009), "The Current State of Internal Auditing: A Personal Perspective and Assessment", EDPACS: *The EDP Audit, Control, and Security Newsletter*, 39(4): 1-23.

[8] Prawitt, D.F., Smith, J.L., & Wood, D.A. (2009), "Internal Audit Quality and Earnings Management", *The Accounting Review*, 84(4): 1255-1280.

[9] PricewaterhouseCoopers (2009), "State of the Internal Audit Profession Study", Retrieved from: http://www.pwc.com/us/en/internal-audit/assets/state_internal_audit_profession_study_09.pdf

[10] Rehage, K., Hunt, S. & Nikitin, F. (2008), "Global technology Audit Guide: Developing the IT Audit Plan", Altamonte Springs, FL: Institute of Internal Auditors.

[11] Ross, J. W. (2003), "Creating a Strategic IT Architecture Competency: Learning in Stages", MIS Quarterly Executive, 2(1): 31-43.

[12] Taylor, J., Allen, J., Hyatt, G.L., Kim, G.H. (2005), "Global technology Audit Guide: Change and Patch Management Controls: Critical for Organizational Success", Altamonte Springs, FL: Institute of Internal Auditors.

[13] Venkatesh, V. (2006), "Where to Go from Here? Thoughts on Future Directions for Research on Individual-Level Technology Adoption with a Focus on Decision Making", Decision Sciences, 37(4): 497-518.