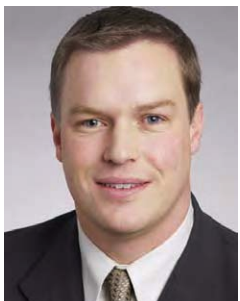


# Application Audits: A Primer for Internal Auditing Professionals



*Technology has become both an enabler of audits and a key operational business factor that must itself be audited. This article will outline specific considerations for internal auditors faced with the challenge of performing application audits.*

*By Michael Cooke  
Practice Leader at  
ACL Services Ltd.*

A maelstrom of market, competitive and regulatory forces, shapes today's auditing landscape. The auditing style of yesterday, with its focus on risk matrices and samples, is quickly becoming outdated as technology rapidly changes the complexion of the auditing environment. Most notably, the pervasiveness of technology has brought with it speed and directness to the auditing world. The fact that audits can now be done on a more continuous and real-time basis has important consequences – technology has become both an enabler of audits and a key operational business factor that must itself be audited.

As a result, successful internal auditors are now faced with a daunting challenge: gaining enough knowledge of information technology, without the benefit of a technical degree or formal training, from which to perform solid and accurate application audits.

Understanding the context for an organization's information system is critical for internal auditors to accurately assess how technology impacts risk, both from a governance and fraud perspective. In addition, auditors must be able to evaluate applications against business process improvements. Though the auditor's ultimate responsibility is to test that controls are valid, timely, complete, authorized, and compliant with regulations, performing an application audit to discover how technology affects each of these factors is a must.

## UNDERSTANDING ORGANIZATIONAL NEEDS: A CRITICAL PRE-AUDIT CONSIDERATION

Before any audit is conducted, auditors must clearly understand the organizational needs of their enterprise, both from an application and business perspective. So which are the top organizational needs that should be accounted for prior to conducting the application audit?

**Regulatory compliance.** The highest profile organizational consideration is regulatory compliance. Sarbanes-Oxley requires senior management to make statements about the effectiveness of internal controls and although technology is a key enabler (because it runs businesses and can help in examining applications across the enterprise), the new law has not determined that continuous monitoring of applications is a 'need-to-have' checkpoint. However, adopting this process can only be a positive step in overall audit quality and business assurance.

**Business operations.** The next consideration that should be examined is business operations critical to the organization. For example, account management in a bank, inventory management in manufacturing, claims processing in an insurance company, etc. They should be considered from the standpoint of system integrity and business performance, evaluating how effectively these business operations are working and assessing their deficiencies. For this area, auditors should insist on implementing a system capable of monitoring applications continuously.

**Corporate governance.** Another area where continuous monitoring is a must is corporate governance. Auditors have a responsibility to shareholders to improve the company's systems, including the ability to report to management, but also more broadly in terms of business process improvements and methods to reduce overhead and budgets.

**Organizational risk.** Finally, auditors should look at organizational risk before an application audit. The auditor must work within the corporate risk program that has already identified the main organizational risks. For example, a financial institution needs to monitor for the secure management of loans and accounts. For telecommunications companies, the ability to monitor the volume and duration of calls and Internet data streams is also a point of focus.

With the organizational needs analysis complete, and the above factors taken into consideration, the examination of specific issues can begin.

## FACTORS TO CONSIDER WHEN AUDITING APPLICATIONS

As I discussed at the beginning of this article, it is important to gain an understanding of the general technology environment. Before coming to grips with an application audit, the internal auditor needs to understand the recent changes in enterprise computing. The key point is that most organizations have been moving from their legacy systems to integrated technology environments. In the past, each department within the company – purchasing, manufacturing, human resources, etc. – would have their own computing systems. Today, these diverse functions are all integrated with business applications or enterprise resource planning solutions (ERP) designed to bring together computing resources across the organization, and thus deliver increased business process efficiency. This is called the integrated business environment – and it creates a whole set of factors that must be evaluated prior to conducting the audit.

At this point, I should note that there are two types of technical audits – infrastructure and application layer audits. The infrastructure audit evaluates operating systems, servers, hardware, user passwords, log-ons, and general computer controls. In the integrated business environment, the infrastructure audit helps ensure that the organization has the right infrastructure to ensure business continuity.

The application layer audit manages the programs and software applications that reside on the technology hardware, such as applications and databases. Email applications and financial applications are examples of the elements that will be audited. The application layer audit is essential in determining that business processes and controls are operating effectively from a financial transaction standpoint.

To do an infrastructure audit you need to be cognizant of a number of (usually historical) factors. For one, in a legacy environment, operating systems generally control access and authentication processes. Also, integrating or analyzing data from multiple legacy systems can be challenging – in fact, some systems (such as OS/390) are difficult to analyze without specialized data extraction tools or custom reports. Because of this, it is advisable to look for tools to assist with auditing operation systems for vulnerabilities. As a further factor where specialist help is advisable, business continuity planning, especially since 9/11, is critical to any organization. In terms of an application audit, there are a number of guidelines to follow and factors that indicate when an application audit is advisable including:

- has the company recently implemented a new application or ERP application;
- has one of the organization's key systems (typically ERP) recently been upgraded substantially;
- has the organization gone through a period of significant downsizing, restructuring or outsourcing;
- how pervasive is computing within the company's transaction-processing functions;
- has the organization recently acquired or merged with another?

## WHAT TO WATCH FOR

In the application audit, the central question is that of personnel and system access. This is of particular concern especially in terms of the new regulations. Sarbanes-Oxley (SOX) 302 says that management must disclose to the external auditor significant deficiencies in internal controls: anything which could adversely affect the ability to record, process, summarize, and report financial data. On top of this, SOX 404 requires management to evaluate the effectiveness of internal controls on a quarterly basis. This means that those who have oversight of internal controls or "employees who have significant roles in internal controls" must be tested and held accountable.

With this in mind, there are several access-related factors that auditors must be aware of during an application audit. First, is the varying levels of user access and their respective responsibilities. There are system administrators with significant privileges, and it is important that they not be given access to transactional processes. Next are super-users with a high degree of access to their particular module and the ability to over-ride controls, and finally standard users with control over specific functions. For the latter two user types, it is important to ensure adequate segregation of duties and that there are no conflicts. For example, no one person must have the ability to both raise a purchase order and to approve an invoice. One problem with such analysis of access is that it is usually done on a 'point in time' basis. If possible, organizations should put in place a system to monitor these functions continuously.

As well as looking at who actually has access to what, a further step in the application audit involves looking at the principles underlying these access levels. An auditor should review the following checklist and ensure that he/she knows:

- who designs and oversees the overall structure of internal controls;
- if the structure has been documented, reviewed, and signed off by management;
- who has the ability to set up or establish application-based internal controls;
- if the system-based controls adequately represent the intentions and objectives of management;
- who monitors the day-to-day administration of the application-based controls;
- how often the controls are reviewed: monthly, quarterly, or annually;
- if control violations are reported, documented, and corrected in a timely fashion;
- whether the review process is manual or technology based – and, if manual, is the allotted time and budget sufficient to mitigate the control risks;
- are violations quantified to give management a clear picture and to allow corrective action?

This can be a complex task. To make it more straightforward, auditors need to gain an understanding of the applications and how they support the business process. Auditors can do this through interviews with operational managers and systems and application administrators. First, try to gain an understanding of the business process flow – how transactions are processed, manually or automatically. Then, identify the risk issues for the business process (for instance, ensuring that valid vendors are established in the supplier master is key to controlling risk in a purchasing process).

Auditors must then understand how it is exactly that the technology enables the business process. Just as with a manual process, they must determine who has the ability to run key control functions such as approve, post, delete, and so on. Some applications may have specific risk issues unique to themselves. In this case especially, research, publications or the use of specialists may be required. Using analytical software to analyze large volumes of data will increase effectiveness and reduce the time-and-effort commitment of such analysis. Other questions to address include: how does the technology operate; how can internal auditors make sure that the applications are working accurately; is the data timely and relevant; and are regulatory laws or compliance issues being met?

## UNDERSTANDING APPLICATION CONFIGURATION IS ESSENTIAL

Once these top-level application audit issues are understood, the auditor must then look at how applications are configured. There are several main elements that need to be taken into account, namely the: data flags/switches; internal control functions; and system administration.

Data structure and flags/switches within an application is a difficult process to undertake and examine, largely because the structure of large systems is very complex. Typically only a database administrator (DBA) will have access to the tables in the applications, so the auditor should first define the testing requirements, then solicit assistance from the DBA. One point to bear in mind, however, is that in most cases system administrators are overwhelmed ensuring the systems are operating efficiently, so assistance may be limited. Be sure to allow some commitment of time and energy to undertake this part of the audit.

Consider also the internal control functions for user access (password, user ids), groups, or profiles that are assigned to that user as they identify where users are going within the application. It is important to note that what an internal auditor may consider a control, a system administrator or super-user may consider functionality. For example, automating the cash disbursement process in a payments process may be core functionality within an application, but configuring the process to only process payments that have been approved by a manager would be a critical control. This distinction is important and often overlooked.

The third point in examining how applications are configured is system administration. Basically, who are the people responsible for assigning administration, and how are they using the application?

As I discussed previously, monitoring changes to user access and roles is a critical, yet a very difficult process without effective control monitoring technologies. For example, a system administrator could assign him or herself self-payment processing functionality, proceed to process some checks, then revoke this access privilege. Typical auditing would not be able to detect this change in access. The potential for problem scenarios like this one is extremely widespread, given that the majority of Fortune 1000 companies will have an ERP system of some sort, and each of these systems have a system administration module.

To address this potential problem, the internal auditor must come to understand the administrative capabilities of this module: who can create roles; and where does the power to create roles lie? It is clear in Sarbanes-Oxley that all companies must be able to provide evidence of fraud from control users: for example, if the vice-president of retail operations is caught skimming revenue, the company must be able to report it, and are obliged to do so by law. Another interpretation of the new law is deeper. It indicates that Sarbanes-Oxley applies also to system administrators as they hold the key to role creation. Such is the potential power of system administrators today, that internal auditors should take care to factor this into their work.

Although there is not sufficient space to review such a large topic here, it should be noted that outsourced systems must also be audited, and that the internal auditor has to include an audit of service providers in their work. However, many service providers don't allow this. SAS-72 (standard auditing standards, ICPA) recommends that auditors conduct a one-time review of service providers. But this doesn't alleviate management's responsibility that controls are in place around the process.

Although all the above can be daunting, it is important for the internal auditor to understand that there are automated technologies available to help them monitor applications and the transactions that flow through the applications. Traditionally, internal auditors fall back to policy review, manual processes and sample analysis, which may fail to meet the requirements of an effective internal audit in a large transaction processing system. New analytical applications are becoming available almost daily to assist internal auditors perform automated, continuous monitoring of ERPs.

## THE INTERNAL AUDITOR AS RISK MANAGER

The final issue we must cover is independence. One trend in the industry is the role of risk manager in which the internal auditor becomes more involved in the risk identification and issue prevention process. Although it is desirable for auditors to provide value to the organization by assisting in the performance improvement, there is a delicate balance that must be maintained to keep the auditor's independence. Clearly, internal auditors cannot design a business process, or implement controls in an ERP. However, with proper diligence they can provide value through the understanding of organizational issues, risks and technology.

Fundamentally, the risk manager and internal auditor are different – the risk manager identifies business risk and works with business managers to proactively manage risk, whereas the internal auditor is typically responsible for examining policies and procedures and ensuring that the operations are functioning within the established policies. The trend with internal auditors is for them to become more proactive in providing input to new operational installations and system installations. The key is to ensure that an internal auditor maintains independence: the ICAPA, CICA and IIA are all clear on the bottom line, which is that no-one should create a system and then audit it.

In summary, the challenges for internal auditors are significant and ever-changing, but help is available. The burgeoning complexity and reach of enterprise-wide application systems has prompted a wide variety of technological answers to address this complexity. There is no question that auditors must work hard to increase their knowledge of information systems and the myriad of ways in which their companies have become dependent upon them. But thankfully, the complexities that new technologies have created can also be solved by technology itself.



### ACL Headquarters

T 604 669 4225  
F 604 669 3557

■ [acl.com](http://acl.com)  
[info@acl.com](mailto:info@acl.com)

AR/AUDNET/MC/E/230504  
Printed in Canada.

Reprinted with permission of AuditNet  
AuditNet, March 2004