IT AUDIT APPROACHES FOR ENTERPRISE RESOURCE PLANNING SYSTEMS

Dr. Richard G. Brody, CPA, CFE, FCPA
Rutledge Professor of Accounting
University of New Mexico

Dr. Grover Kearns, CPA, CFE
Associate Professor of Accounting
University of South Florida St. Petersburg

INTRODUCTION

Because of their integrated nature, enterprise resource planning (ERP) systems have become popular among firms of all sizes. This system-wide integration changes the ability of and need for auditors to perform substantive tests. The proliferation of ERPs makes it imperative that auditors become knowledgeable about the various controls and recommended audit approaches that should exist for these systems. Now, auditors must rely less on auditing around the computer and develop sufficient technical expertise to allow for auditing through the computer and with the computer. Finally, auditors must familiarize themselves with the underlying business processes and obtain assurance that the system reflects them accurately. Without the proper tools and expertise, control risk may be underestimated and the possibility for significant misstatements and fraud elevated.

This paper examines the special issues ERP environments create for auditors and the recommended approaches for controlling risk. The remainder of the paper is organized as follows. First, ERP is explained followed by a description of audit issues in an electronic environment. Next, specific steps for the ERP audit are presented. Finally, conclusions are drawn about the distinctiveness of ERP audit techniques.

ENTERPRISE RESOURCE PLANNING (ERP)

ERP systems have the capability of integrating virtually all business processes by installation of program application modules for sales, marketing, accounting, finance, production and materials management, and human resources (Jacobs & Whybark, 2000). These systems use a common database for all accounting and operating information instead of relying on separate
master files found in batch applications. Many companies do not implement all of the available modules preferring to “bolt-on” legacy systems that are viewed as best practices. ERPs are usually client-server networks that operate across multiple platforms. Some systems, such as the SAP R/3, offer an open-architecture that allows other software vendors to tailor their applications for tighter integration (e.g., Brady, Monk, & Wagner, 2001; Jacobs & Whybark, 2000).

Major vendors of ERP systems include SAP, Oracle, PeopleSoft (now part of Oracle), Baan, and J.D. Edwards. Because of the advantages of integrated processing and a common database, companies frequently implement ERPs prior to implementations of other major applications such as customer relationship management systems (CRMs), supply-chain management systems (SCMs), and data warehouses. Because the high complexity and revisions to business processes, changes to the organizational structure are usually necessary. Without proper project management, employees may resist the introduction of ERPs. For these reasons many firms have failed in their efforts to implement them successfully or cancelled the implementations altogether resulting in sizable losses (e.g., Parth & Gumz, 2003; Schwalbe, 2006). Arizona State University introduced an Oracle ERP system on a fast-track by recognizing problems were going to occur by maintaining a rigid schedule. They maintained, however, that the problems were offset by the cost savings reaped by early introduction (Worthen, 2007). The approach created nightmares for employees and vulnerabilities to internal control.

INTERNAL CONTROL IN AN ELECTRONIC ENVIRONMENT

Auditors must develop an understanding of the firm’s internal control structure and the effectiveness of the controls in order to evaluate the assertions. Examination of the types of controls can reveal insight into the types of financial misstatements that might occur (Senft, Manson, Gonzales & Gallegos, 2004).

When auditors focus on financial statement assertions, attention is given to how transactions are authorized, recorded, aggregated and reported. All financial audits should consider the firm’s demographics including size, industry, legal and regulatory requirements, and organizational structure. Because the majority of firms are highly dependent on electronic accounting information systems, special attention must be given to the system controls and information technology (IT) environment. The following discussion of IT auditing for ERPs is summarized in Figure 1 which captures the main decisions an auditor will face.

**IT Auditing**

IT auditing involves examination of the general and application controls present in the IT environment. Computers affect both interim and financial statement audits in several ways. Auditing around the computer ignores the actual processing. It essentially compares the data inputs with the information outputs from the processing. Knowledge of what steps are supposed to occur in the processing will allow creating an expected test version of the output for comparison. Auditing through the computer focuses on the verification of general and application controls in the IT environment. This requires knowledge of specific applications and may even require direct examination of computer code. Attention is given to the overall security of the IT environment and overall data integrity. Auditing with the computer, on the other hand, makes use of various audit software packages, known as generalized audit software (GAS), to make the process of retrieving and analyzing data more efficient. This may require a software specialist if the audit staff is not familiar with the programs or the analytical methods. GAS packages such as ACL support computer-assisted audit techniques (CAATs). They can be used for testing automated controls, data related to assertions, and the effectiveness of access controls.
All three of these computer-based approaches may be present in an ERP audit (Bodnar & Hopwood, 2004).

GAS and CAATs are also effective instruments for ERP fraud investigations using techniques such as discovery sampling and computer searches (Albrecht, Albrecht, & Albrecht, 2006).

**Computer Forensics**

Because of the number of transactions processed by ERP systems and the real-time nature, fraud examination methods employed in other systems must be augmented. Computer forensics is the investigative process that seeks to determine if computers and other data storage devices have been used in fraudulent activities. Although not necessary in all audits, the complexity of ERP systems may require the use of a forensics expert when fraud is suspected. In fraud examinations, it is important that the auditor know how to “freeze the scene.” For example, the auditor should unplug the computer rather than shutting it down. Shut-downs erase temporary files and evidence of user activity. Forensic experts can discover all data files including hidden and even deleted files on disks. This requires a technical understanding of the physical disk layouts and the use of forensic tools (Schwalbe, 2006).
Figure 1. Significant Audit Steps for an ERP Environment

START

Audit ERP Physical Security

Review Super User Access Rights

Review Audit Logs

Fraud Suspected?

No

Yes

Freeze Site Use Forensics

Recent ERP Installation?

Yes

Review Subschemas, Access Matrix, Security Settings

No

Separate Legacy Applications?

Yes

Audit LA Around Computer

No

Bolted On Applications?

Yes

Audit Bolted On Separately

No

Audit ERP Through Computer

Large or Nonroutine Items?

Yes

Audit With Computer

No

Control Risk Acceptable?

Yes

END

No

Increase Substantive Testing
Audit Risks

In audits, there is a risk that a material misstatement in a financial statement assertion will not be prevented or detected by the firm’s internal controls. This is known as control risk. The risk that such misstatements will not be uncovered during the audit is detection risk. Errors that exist prior to the application of controls are inherent and the probability of their existence is inherent risk. Control risk and inherent risk can be used to determine the acceptable level of detection risk. For lower levels of detection risk, increased levels of assurance should be provided by substantive tests. Conclusions for the assessed level of control risk must also be documented. The extensiveness of documentation about internal controls should be in direct proportion to the controls themselves. For example, if the auditor asserts that the control risk is below the maximum, documentation should provide direct support by the inclusion of the specific items that reduce risk.

For audits of ERP systems, detection risk will be highly dependent upon the skill and expertise of audit staff and their knowledge of the underlying business processes that are integrated into the system. Lack of expertise could lead auditors to conclude that output from the system was correct when, in fact, some problems existed in the application programs that produced erroneous results. Lack of expertise might also lead auditors to conclude that segregation of duties is reasonable when, in fact, certain users have incompatible access privileges to the data base that increases the potential for fraudulent activities.

Environments with large accounting information systems are highly complex and SAS 94 prescribes attention to the design and implementation of controls as well as substantive tests in order to reach the required level of control risk. The absence of the control tests may warrant a scope limitation and prevent the issuance of an opinion on the financial statements (Ratcliffe & Munter, 2002). Four steps are necessary in order to assess control risk below the maximum.

1. Identifying internal controls that can prevent or detect material misstatements related to assertions,
2. Evaluating effectiveness of controls through tests,
3. Determining the assessed level of control risk, and
4. Documenting the assessed level of control risk.

The Control Objectives for Information and Related Technology (CobiT) identifies 318 control objectives for IT. Developed by the IT Governance Institute and the Information Systems Audit and Control Foundation in 1992, CobiT has gained wider recognition and acceptance since the passage of the 2002 Sarbanes-Oxley Act. CobiT is accepted as good practice for control over IT and related risks and it is important that firms implement its guidelines in order to achieve effective IT governance (IT Governance Institute, 2004). Generally, it comprises critical success factors, performance measurement elements, and maturity models.

In certain cases, the auditor may determine that substantive tests alone provide the best approach. When audits are limited to fixed assets and long-term debt, for example, transactions can be readily corroborated and substantive tests would provide reasonable assurance for assertions.

Accounting Statements Impacting IT Audits

The AICPA, with input from major accounting firms, has issued statements that provide guidance for audits that depend on electronic evidential matter. A brief discussion follows.

SAS 78 defines internal control in terms of the “COSO” model (see Table 1). The model defined internal controls as consisting of five components: the control environment, risk assessment, control activities, information and communication, and monitoring.
SAS 80 defines evidential matter to include both written and electronic information developed or available to the auditor that assists in the formation of an opinion. Electronic documents may be similar to the paper equivalents but it is often the case that source documents are replaced by electronic messages such as with electronic data interchange (EDI). Also, electronic evidence may be transformed or change physical location during backups. SAS 80 notes that the auditor must consider this when developing the nature and timing of the audit.

SAS 94 notes that the impact of IT on each of the five components in the COSO model must be considered in the audit. It also notes that IT may reduce the visibility of activities particularly with the automated entry of data at point-of-sale by the use of bar codes and scanners. (The increasing use of radio frequency identification devices (RFIDs) will heighten automated data entry especially for inventories.)

The processes by which transactions are initiated, recorded, and processed are also altered by IT. Controls in the IT environment can be embedded within the applications or depend on manual implementation. It is especially important to assess the overall level of control when systems are in transition. Transitions can leave the company vulnerable to either material misstatements or fraud if internal controls were not designed properly for the new system or if a highly complex system (such as an ERP) was introduced without sufficient attention to revision of existing internal controls. Greater attention must also be given to automated or embedded controls in new systems to ensure they are operating properly. At the same time, the understanding of system users must be evaluated to determine if they are able to handle both routine and nonroutine activities.

SAS 94 further notes that the IT environment may reduce the need for substantive testing. Audit risk may be minimized by first assessing the IT controls and then limiting substantive tests to significant amounts and transactions that are manual or nonroutine.

In its Auditing Procedures Study, The Information Technology Age: Evidential Matter in the Electronic Environment, the AICPA noted several challenges to audits that rely on electronic evidence. Electronic evidence can be altered more easily than its paper equivalents. Electronic documents may be incomplete as to information where codes and/or cross references substitute for actual information such as addresses, item names, etc. Approvals on electronic evidence may not be as apparent or conclusive. Electronic evidence is not readily available and may require technical support for extraction. Thus, when working with electronic evidential matter, it is more difficult to establish credibility and tests specific to the system must be performed by knowledgeable staff with an understanding of the embedded system controls. Table 1 summarizes the accounting statements and reports that impact IT audits.
Table 1. Accounting Statements and Reports Impacting IT Audits

<table>
<thead>
<tr>
<th>Source</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AICPA</td>
<td>Auditing &amp; EDP (1968). The big eight accounting firms participated in the development of this book that described how to process internal control reviews and document EDP audits.</td>
</tr>
<tr>
<td>SAS 3</td>
<td>The Effects of EDP on the Auditor's Study and Evaluation of Internal Control (1974)</td>
</tr>
<tr>
<td></td>
<td>Control Objectives for Information and Related Technology (CobiT) 1977 by the EDP Auditor’s Association. Included guidelines, procedures, and standards for EDP audits. EDPAA changed its name to Information Systems Audit and Control Association (ISACA) in 1994.</td>
</tr>
<tr>
<td>SAS 78</td>
<td>Consideration of Internal Control in a Financial Statement Audit: An Amendment to Statement on Auditing Standards No. 55. (1995) Incorporated “COSO” model approach to internal controls which were described as providing reasonable assurance of reliable financial reporting, effective and efficient operations, and compliance with applicable laws and regulation.</td>
</tr>
<tr>
<td>SAS 80</td>
<td>Amendment to Statement on Auditing Standards No. 31, Evidential Matter (1996) Addressed problems of auditing firms that depend on electronic processing of information. Concluded that in such environments auditors might not find it practical or possible to rely only on substantive tests of financial statements. Instead, tests of control combined with substantive tests would be sufficient to support an audit opinion.</td>
</tr>
<tr>
<td>SAS 94</td>
<td>The Effect of Information Technology on the Auditor’s Consideration of Internal Control in a Financial Statement Audit (2001). Offers guidance on audits in an electronic data processing (EDP) environment including collecting sufficient, competent evidence. Identifies circumstances where EDP system controls must be assessed. Amends SAS 55 and expands SAS 80. Addresses the effect EDP has on internal controls, the auditor’s understanding of internal controls, and the required assessment of control risk.</td>
</tr>
<tr>
<td>SAS 99</td>
<td>Consideration of Fraud in a Financial Statement Audit (2002). Supersedes SAS 82 and was issued partly in response to recent accounting scandals. Incorporates recommendations from the PCAOB and other contributors including the International Auditing &amp; Assurance Standards Board. Describes the fraud triangle, emphasizes risk assessment, internal controls to mitigate identified fraud risks and significantly extends the documentation requirements.</td>
</tr>
</tbody>
</table>
THE ERP AUDIT

Each ERP system is distinctive reflecting the individual client’s particular integration of modules, legacy systems, and customization. Most ERP systems are modular which allows companies to select which integrated processes to implement and also to bolt-on existing legacy systems they wish to retain. This customization plus the tailoring each company performs to make the ERP firm-specific presents a challenge to the auditors who must gain an understanding of the overall processing relationships in order to analyze the underlying controls.

A user access matrix will be established by the client giving individual users rights and privileges that may or may not support full segregation of duties. Individual users should be restricted to subschemas of the ERP database that have been carefully designed to avoid incompatibilities. Users who only need to view information should not be given write-access to files.

Auditors must verify financial reporting and internal controls by operating through the computer. This requires an extended competency: an “integrated auditor” who has both audit and computer competencies (Hahn, 1999). An alternative is to use outside expertise by engaging a specialist. At a minimum, auditors should have access to a specialist who can read and interpret the computer code (Hahn, 1999).

In ERP systems, paper audit trails are replaced by automatically generated audit logs that provide supporting entries (Adint, 2002). The quality and extensiveness of the log will help determine the extent to which the auditor can rely on system controls. Most ERP systems perform audit checks and generate internal audit logs (Finnigan, 2003). Additionally, integrated legacy systems may require auditing around the computer by checking inputs to outputs to verify the accuracy of processing for those applications. Unlike batch systems, ERPs are online and real-time meaning that changes are reflected through all of the accounts immediately. Data entry may be made from various locations without data checking. For these reasons, financial audits in ERP environments must be made through the computer using a test data or parallel simulation approach. To do so requires an understanding of the underlying business processes captured in the system.

By modifying programs in ERP systems, extended records are created that provide additional data not normally collected to selected transactions. By tagging these transactions, the processing steps are added to the extended record providing a step-by-step audit trail for the process (Bodnar & Hopwood, 2004). Summary statistics can be provided using special mapping software that will allow auditors to determine the number of times program statements have been executed. Using test data combined with mapping, auditors can determine which statements processed the data.

ERP systems, when implemented, replace a number of existing legacy systems and the controls over those systems. Implementation of revised internal controls may lag the actual system implementation making the ERP more vulnerable. Also, when delivered and initially installed the ERP security features are turned off to allow for ease of system access during testing. When moved into production, it is essential that all security settings be activated and reviewed for effectiveness. After installation, continuous monitoring is necessary because the ERP may have multiple points of vulnerability and the majority of the firm’s information now resides on a single database.

ERP Audit Scope
Financial reporting with ERP is streamlined to the extent that many firms can and do close their books daily. Using online transaction processing (OLTP) capabilities, ledgers, summaries, and financial statements can be prepared for internal and external users. The loss of batch controls and reduced reliance on audit trails increases the emphasis on data entry checks and transaction validations (Hall & Singleton, 2005).

ERP audits are concerned primarily with the adequacy of security, data integrity, and employee training. Determining the adequacy of controls within the system is necessary in order to determine the existence of material deficiencies in system controls.

The scope of an ERP audit will be dependent upon (1) the level of system security, (2) the specific ERP modules implemented, (3) the legacy systems that have been “bolted-on”, (4) the user access matrix with specific permissions and privileges, (5) super-user access rights, and (6) the extent of employee training.

**ERP Security Auditing**

Security is a major control risk for ERP systems and auditors should determine whether the security standards framework for the ERP system meets the standards for the firm’s security policy (IT Governance Institute, 2004). ERP security audits should focus on physical access, system access, and segregation of duties. Physical access is the easiest to ascertain and includes access to data centers, data libraries, and servers.

When originally implemented, ERP security controls are not activated. For newer installations, the auditor should check to see if these controls have been properly activated and that security settings are correct. User access profiles can be reviewed to ensure proper segregation of duties to minimize the opportunity for fraud. SAP audit functions provide the capability to compare actual user access against the matrix of allowable accesses (Moulton, 2005). Also, data subschemas should reflect job responsibilities and provide for sufficient segregation of duties.

Segregation of duties within a highly integrated accounting information system is accomplished by restriction of access rights. For example, employees who have the right to enter new vendors should not be able to initiate a purchase requisition or purchase order.

ERPs change organizational structures and the way organizations do business. An important control issue is how supervisory roles are altered by ERPs. When implemented, many decision-making responsibilities are reoriented to lower level employees. Although spans of control will increase because of efficiency benefits, supervision should remain an important component of internal control assisted by improved monitoring capabilities (Hall & Singleton, 2005).

Permissions, rights, and privileges for access to data should be evaluated to insure that passwords are sufficiently strong and changed at least monthly. Audit controls should be highest for super-users and other users who have access to sensitive areas or extensive modification rights. User access profiles should be created to segregate incompatible duties and documented and logs should be reviewed regularly to insure that unauthorized users have not accessed the system. Controls over the addition of new users should include proper training that reflects an understanding of company security policies. Profiles for terminated employees should be updated immediately upon termination to remove all access rights.

One way SAP overcomes the problem of segregation of duties is to define “user roles” which establishes a set of activities associated with a specific user and defines access rights.
Over 150 predefined user roles are provided by SAP and these can be customized to reflect unique needs of the firm (Jacobs and Whybark, 2000).

The audit should also address the security features that are activated for the firm’s operating environment. Conditions of poor security increase the likelihood of fraud and represent a material weakness that should be included in the auditor’s report. The Center for Internet Security publishes the specific settings and downloadable software for checking system settings (see http://www.cisecurity.org). Because ERP systems are always available and may be accessed from various geographical locations, sometimes at any time of day, continuous monitoring is essential. Logs should provide not only access identifications but time and place of access. CAATs can be used to determine if systems accesses are abnormally high or the location is inappropriate.

ERPs are especially vulnerable to cybercrime. In a sense, ERPs place all the eggs in one basket. Whereas network attacks can only target individual legacy systems, an ERP database can contain the majority of a company’s operating and accounting information. Malicious attacks that spread viruses or deny service can shut-down systems for hours or even days (Crumbly, Heitger, & Smith, 2005). For these reasons, special emphasis must be given to continuous backups of databases and network security. Off-site backups for incremental changes to databases can be accomplished over the network on a daily basis. Full backups should be performed periodically and maintained offsite.

**Data Integrity Auditing**

Transaction authorization is vital to data integrity in ERP systems. The benefit of the tightly integrated modules creates potential problems for transaction authorization. Because of the real-time nature of processing, controls must be present to validate transactions before they are accepted by the system. Many of the controls are programmed within the system and the challenge to auditors is to gain a detailed understanding of the controls and ensure they are being used (Hall & Singleton, 2005). Benefits of ERP are numerous. Automated quality-assurance testing is available for every transaction without disruptions caused by traditional auditing methods. Many audit programs run concurrently with normal processing to capture audit data and identify errors as they occur (Taylor, 2006).

Most ERP systems integrate data from legacy systems. Auditors must have an understanding of the process and know the source of the data, the points of processing, and the points of integration. Some systems provide for the use of embedded audit routines that the user can customize. Snapshots can be used to provide detail about specific processing functions. Auditors must verify the existence and effectiveness of backups of output and disaster recovery plans. Off-site backups should occur at regular intervals and training for disaster recovery should be evaluated.

Changes to program code should be authorized and documented internally within the code as well as externally. Controls should separate program coding changes from program execution and access to related data files. Testing of all changes should be documented and reviewed before the revisions are placed into production. If testing is not given high priority, errors might go undetected causing serious weaknesses in the accounting information systems and in financial reporting.

Control requires continuous monitoring of system access and a log of all access activities. The functions of development, testing, and production should be separated. Development, other than routine maintenance, should be initiated and approved outside of the IT function. Personnel
responsible for modifying code should not be able to place code into production or execute production code. Similarly, access to data libraries should be separated from operations to prevent fraudulent changes to data (Perry, 1985). All changes to code should be tested, documented and reviewed prior to placing it into production (Adint, 2002).

In addition to auditing through the system, audits around the system should ensure that results from ERP processing are reconciled to external information such as bank statements. High priority should be given to vulnerable areas such as accounts payable. Controls for responsibility accounting centers must be reviewed and the authorization process for nonroutine transactions.

ERP systems can be implemented for any size company and the underlying control environments can be unique and complex. Examination of various internal checks such as the use of check digits, cross-field checking, limit tests, table lookups, and default values can help to establish data integrity (Hahn, 1999). Attention must also be given to the specific points of data entry including automated entry at point-of-sale and EDI. Data entered from purchase requisitions, purchase orders, invoices, and invoices are posted immediately throughout the system and correction of errors will be more pervasive than with stand-alone legacy systems (Brady, Monk & Wagner, 2001).

Employee Training

Data integrity in ERP environments is highly dependent on how well lower-level employees who enter the data understand their jobs and the system. For this reason, time should be spent interviewing these employees and documenting their ability to deal with regular and irregular work situations. Because ERP systems are highly sophisticated, employee training procedures should be reviewed including the proficiency level of employees, training schedules, and how system changes and new modules are introduced (Brady, Monk & Wagner, 2001).

ERP systems require greater training to master duties and responsibilities and can represent a significant investment for employers. For this reason, employees are often undertrained which can introduce opportunities for errors and fraud. Data accepted by the system is posted through all accounts immediately and errors become pervasive. Employees must be trained to deal with “nonroutine and nonsystematic transactions, such as accounts involving judgments and estimates” (IT Governance Institute, 2004, p. 37).

Working Papers and Documentation

Auditor’s working papers should include documentation of the company’s business processes that are captured by the ERP and legacy systems. Documentation may consist of narratives, flowcharts, and graphics such as data-flow-diagrams, entity-relationship diagrams, and resource-event-entity models. It is important that auditors have an understanding of the graphical methods in order to determine if the described relationships and processes accurately reflect the actual processing of information. Furthermore, it is necessary in order to determine if individual user rights and privileges reflect the appropriate segregation of duties (Cooke, 2004).

Electronic working papers can improve both the quality and consistency of audit working papers. By providing current and archived working papers in a centralized audit file, auditors can more easily coordinate concurrent audits and consider findings from prior or related audits. Text files, spreadsheets, graphics, slides, and databases may comprise electronic working papers. Management of these files may be supported by a commercial software package developed specifically for IT audits. The use of intelligent work papers can save time in documenting
responses to internal control questionnaires wherein answers are automatically logged and potential weaknesses identified in a section of the audit report. Problems to other areas of the audits can be logged by individual staffers during the project so that the supervisor is kept informed of the ongoing status and can focus attention on problem areas.

Good documentation is even more important for ERP systems than legacy systems. Because more reliance must be placed upon electronic sources, reliance upon supporting documentation is critical. Good documentation serves a variety of purposes (Bodnar & Hopwood, 2004). It is the basis for employee training, it provides IT programmers and analysts information for future modifications, it provides auditors with support for evaluation of internal controls, and it helps to assure that the systems design specifications were correctly implemented (Bodnar & Hopwood, 2004).

IT audits, particularly in ERP environments, require the retrieval of significant amounts of data from the firm’s files. Some data may reside on direct access data devices such as hard drives. Other data may only be available on sequential access devices such as magnetic tape. Data may be stored in multiple files and multiple formats. Expertise is necessary to access the data and make it available for analysis. One approach is to use commercial products designed for data retrieval. Underlying knowledge of these products is necessary. Further technical assistance may be necessary where these products are not adequate for all applications. Some auditors rely on the use of query languages such as SQL which can be tailored to the firm’s data files if the technical expertise is available. Libraries of commonly used retrieval routines should be maintained for use in future audits. Sections of previous audits can be copied saving time and labor. Key word indexing for these libraries can be used to provide for search engine queries. For repetitive, standard analysis, the routines may be used remotely online and save on travel expense and time.

Longitudinal analysis using CAATs has the advantage of revealing trends, patterns, and shifts in the data. Changes revealed by this pattern analysis may indicate problems that require the attention of the auditor. For example, large increases in accounts receivable without related increases in revenues or large increases in purchases from a single vendor when that vendor’s prices are not significantly lower may indicate suspicious transactions or simply poor management. An understanding of analytical techniques, such as Benford’s Law, is required for examining these patterns (Albrecht, Albrecht, & Albrecht, 2006).

Automated monitoring through embedded audit tools can be very sophisticated if the company has implemented these tools. The auditor should inform management if these tools are not adequate or if greater benefits could be derived from extending them. Internal control will be enhanced if monitoring provides higher quality feedback and allows both management and auditors to turn their attention to areas of greater risk such as accounts payable, payroll, expense reporting, and inventory management. Automated tools can also assist in identifying patterns that hint at fraudulent activities such as excessive expenses, duplicate payments, invalid vendors, low inventory turnover, shrinkage, and payments to terminated employees.

Audit information can be quickly distributed electronically over the Internet or by posting to a Web site. Data confidentiality should be assured by password protection and sensitive data encrypted. Assessments of control vulnerabilities should be considered especially sensitive because it represents a risk element and could support fraudulent or malicious conduct.

CONCLUSIONS
The increased reliance on IT in business has shifted auditor’s reliance on substantive evidence to an emphasis on controls over accounting information systems. Evidence should assure that these controls are being monitored continuously with corrective actions taken whenever events occur. The increased reliance on highly integrated ERP systems increases the role of automated audit routines, electronic transaction logs, and data file interrogation. To provide an acceptable level of control risk, auditors must produce supportive evidence to provide reasonable assurance of systems security and data integrity as well as provide substantive tests in other areas. Transaction validation and continuous monitoring are essential. Audits of firms with ERPs should incorporate the use of auditing through the computer techniques and, where legacy systems are in use, audit around the computer techniques. GAS and knowledge of CAATs are indispensable. For these reasons, IT audits require an auditor with extensive training in IT or availability of technical expertise.
REFERENCES


