NORTHERN ILLINOIS UNIVERSITY

The Impact on the Internal Audit Department When An Entity Implements a New Accounting System or New Accounting Software

A Thesis Submitted to the
University Honors Program
In Partial Fulfillment of the
Requirements for the Baccalaureate Degree

With University Honors
Department of Accountancy

By
Pamela J. Hector
DeKalb, Illinois
December 17, 2000
Capstone Title: (print or type):

"The Impact on the Internal Audit Department When an Entity Implements a New Accounting System or New Accounting Software"

Student Name (print or type): Pamela J. Hector

Faculty Supervisor (print or type): Dr. David H. Sinason, C.P.A., PhD.

Faculty Approval Signature: 

Department of (print or type): Accountancy

Date of Approval (print or type): February 5, 2001
ABSTRACT: The purpose of this paper examines how the internal audit department is affected when a company implements a new accounting system or new accounting software. A change in accounting systems can put the integrity of the data at risk, thus increasing the potential for a material misstatement in the general ledger and subsidiary accounts. This study focused on changes to the internal audit department’s daily routine, including the assessment of risk and the internal controls of the new system. Using an open-ended questionnaire, six auditors, each from a different company, were surveyed as to their experiences after implementing a new accounting system or new accounting software. Companies were selected based on their willingness to participate and guaranteed anonymity to assist in obtaining full disclosure and accuracy.
The Impact on the Internal Audit Department When An Entity Implements a New Accounting System or New Accounting Software
Acknowledgements

I would like to acknowledge all of those who participated in the research for this project. I greatly appreciate the time and effort they devoted to this survey as well as the support of their respective companies. Without their generosity, this project would not have been possible.

I would also like to express my gratitude to the Department of Accountancy and the College of Business, in conjunction with the Honors Department at Northern Illinois University. Thank you for providing me with the best possible curriculum and the very gifted instructors that have made this experience so very meaningful for me.

Most importantly, I would like to extend my sincerest appreciation to Dr. David H. Sinason, Ph.D., C.P.A., C.F.E., C.F.S.A. for his support and encouragement as my professor, advisor and friend.

Pamela J. Hector
Introduction

Since the installation of new accounting software at the company where I am employed, I have been unable to reconcile some of the funds for which I am responsible. This frustrating experience lead me to wonder if this type of situation is prevalent among companies that implement new accounting software. More specifically I questioned whether a conversion of this type would increase the risk of errors in subsidiary account balances that potentially could aggregate into material misstatements in the general ledger.

Preliminary Discussion

The Responsibilities of the Internal Auditor

The internal auditor's role is that of an overseer hired by management to ensure the operational goals of the company are being met and to report to management any situation where improvements could be made to achieve those goals. The internal auditor's primary activities are to conduct compliance and operational audits within their organization. As such, any irregularity not discovered immediately by line personnel should be detected by the internal auditor and reported to the appropriate party for corrective action (Wallace & White, 1994, p.19). Unlike an external auditor who's role is to issue an opinion on a company's financial position at a specific point in time, the work of the internal auditor is a process (p. 17), an ongoing report to management as to the economic status and control systems' soundness of the company.
Like the external auditor's report on the financial position of a company, the evaluation and report on the controls for a particular system are related to a specific point in time. The auditor must evaluate or reassess the level of risk associated with the internal controls. Subsequent reports on internal controls could be vastly different due to any changes that may occur within a reporting period. Such changes may include the reassigning of duties, the addition of new personnel, or changes to the technology utilized by the company. Changes of this type imply increased risk and should cause the auditor to reevaluate the assessed level of risk. If the level of risk is determined to be higher, the auditor will increase testing. It is the ongoing internal control process, however, that allows management to place the utmost trust in its internal audit function. Furthermore, as members of the Institute of Internal Auditors (IIA) a responsible internal audit team (as well as other accounting professionals) will refer to the Committee of Sponsoring Organizations of the Treadway Commission Framework as authoritative guidance for meeting management's objectives. The COSO executive summary states, in part, "Internal control is broadly defined as a process, effected by an entity's board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of (management's) objectives." The objectives include effectiveness and efficiency of operations, reliability of financial reporting and compliance with applicable laws and regulations (Wallace & White, p.11; Committee of Sponsoring Organizations of the Treadway Commission [COSO], 1992).
Auditors, whether internal or external, must have the ability to appropriately choose among alternative procedures in order to achieve organizational goals.

Organizational goals can be defined as "maximizing profits." When changes in technology occur within the organization, the internal auditor must be able to discern 1. who will perform the tests (which personnel are best qualified), 2. what tests should be performed (test data, parallel simulation, etc.), 3. when should the tests be performed (before, during, after implementation) and 4. how many tests should be performed (in order to provide reasonable assurance). Management will expect the internal audit department's choices to be based on cost-benefit analysis and the internal auditor should strive to achieve the cost-benefit of efficiency and effectiveness when evaluating internal controls. However, cost-benefit analysis can lead an organization to de-emphasize internal control because the costs of control procedures are easily quantified, the long-term benefits are more difficult to quantify (Frigo, 1995, pp. 10 &11). The question becomes one of materiality and risk. When implementing a new system, whether electronic data interchange (EDI), electronic funds transfer (EFT) or one of the accounting software systems such as Peoplesoft or Banner, the goal is to minimize error (risk) and increase efficiency and effectiveness.

The Affects of Technological Change on the Business Environment

Since the development of the first computer system, technology has penetrated every facet and function of the business environment. Many technologies (word processing, computerized billing) have been developed to enhance business
operations and profit maximization, and many businesses (AOL, US Cellular) have been created because of the technologies available today. Companies are continuously implementing new or upgrading existing technologies. Each technological change implies a risk (loss) to the company implementing the change, yet businesses are increasing the number of technologies they implement. Frigo's study (1995) examines the use of business process reengineering (implementing technological changes to every department) among hundreds of US companies. Frigo described business process reengineering (BPR) as "the radical redesign of business processes to achieve improvements in critical measures of performance, such as cost, quality, service or speed" (p. 9). Over 75% of the participants of this study said their companies had initiated or had already fully implemented BPR. Considering the total amount of technological changes implemented, it would follow there would be a significant increase in risk. One of the findings of this study showed that while 51% of companies reported improved efficiency (reduced cost), only 21% reported improved effectiveness (control) (p. 2). The model for risk assessment demonstrates that decreasing the effectiveness in the internal control process will increase the level of risk.

For companies implementing BPR, including new accounting systems or accounting software, serious concerns should be raised. Since only 21% of Frigo's participants indicated improved effectiveness with BPR, there remain over 70% who either disagree or are still uncertain. Yet when asked about the impact on their companies, those internal auditors surveyed by Frigo did not believe that the internal controls
which had been eliminated with BPR should be reinstated (pp. 3, 37). It would have been more logical for one to conclude that because a significant number of the internal auditors were not satisfied with the level of internal control achieved with BPR and that they would have increased their assessment of risk. The level of risk assessment must increase whenever control decreases. That is not to say that errors or misstatements are present when BPR occurs, only that the potential for them increases.

The Affects of Technological Change on the Role of the Internal Auditor

Over 78% of the participants in the Frigo study reported that they had served as consultants and advisors to their companies pursuing BPR (pp. 4 & 38). Yet a member of my company's internal audit department disagrees and states specifically that "in order to maintain his independence, his role is to provide assurance based on whatever system or evidence he was given, and not that of advisor as to what system to implement." When a company is selecting a new accounting system, the loss of independence on the part of the internal auditor during the selection process could increase the level of risk to a company. Both the Generally Accepted Auditing Standards (GAAS) and the standards set by the Institute of Internal Auditors (IIA) require an auditor to maintain his or her independence. Given the dependence of the internal auditor on his employer, however, some professionals claim it is not possible for the internal auditor to remain truly independent (Frigo, pp. 5 & 17).
As new systems are implemented, one of the significant impacts on the internal audit department is to outsource its function. As technology continues to evolve, the internal auditor must possess even greater technological ability. If this knowledge will cost the company more money in terms of hiring qualified personnel, the company may find outsourcing that function is more cost effective than upgrading its staff (p. 4 & 55). Having access to the most knowledgeable auditing personnel is one way in which companies can minimize their risk.

Another impact on the internal audit department is a shift in the mindset of the internal auditor. The characteristics of the ideal internal auditor are changing.

Another study by McNamee and Selim (1998) will show this to be true as well. For now, however, the Frigo study listed the following as necessary and "desirable traits of the internal auditor in reengineering:

- Being proactive.
- Being open-minded about alternative controls in reengineered processes.
- Being independent without being rigidly independent.
- Working in interdisciplinary teams and developing new skills.
- Value-added orientation.
- Shifting from a detective to a preventive audit orientation.
- Focusing on processes and process improvement.
- Recognizing that quality, efficiency, and control go together (pp. 5 & 39-40)."

Business Process Reengineering can be analogous to the proverbial two-edged sword for the internal auditor. Frigo points out,

"BPR represents both an opportunity and a threat to internal auditors. The opportunities are significant in that internal auditors can add value by becoming part of the BPR process and can ensure that internal controls in reengineered processes are both
efficient and effective. BPR can be a threat to internal auditors if they do not get involved in the BPR process and allow processes to be reengineered without adequate consideration of internal controls" (pp. 7 & 45).

The internal auditor can never lose sight of the internal control process. While efficiency and effectiveness are still the goals of management, the internal audit department will be more concerned with effectiveness. The auditor has various means for evaluating internal controls. In a test of controls, computer assisted audit techniques can be used. These include test data, parallel simulation, ITF (integrated test facility) and embedded audit modules (Boockholdt, 1999, p. 488). Generalized audit software, or GAS, is a software package developed to aid in performing common audit tasks. Many of the major CPA firms have developed their own software. One such example is INFUCUS (Information and Control Understanding System) developed by Grant Thornton, LLP. This software is able to document and evaluate the system of internal accounting procedures and controls related to various significant accounting cycles in a financial reporting system (Frigo, pp. 31-32).

McNamee and Selim (pp. 2-4) examine other affects on the internal auditor. The internal auditor has changed or shifted his focus over the past fifty years. Furthermore, this is not the first shift recorded for the profession. The first internal audit paradigm focused on observing and counting. The second paradigm was a system of internal controls. This system of internal controls has been applied widely since its introduction in 1941 by Victor Brink. McNamee and Selim now believe the
internal audit focus to will be on risk. For purposes of this study the authors defined risk as, "a concept used to express uncertainty about events and/or their outcomes that could have a material effect on the goals of the organization."

This latest change in focus is seen as a response to the significant and rapid change in internal auditing from that of passive and reactive control-based to one of active and anticipative risk-based auditing. According to this study, risk-based auditing has become evident throughout the profession. By exchanging the word risk for the word control in the auditor’s vocabulary, the focus of the internal auditor has changed once again. Internal auditors are using risk management principles to change the way that they plan and report audits. Moreover this new vocabulary makes it easier for line managers to buy into the goals of the internal audit department as these managers can understand what risk means to their divisions but resist the concept of being controlled.

The Affects of Technological Change on Audit Reporting

The assurances rendered by the internal auditor to management and the internal audit committee can be paramount in providing information to the external auditor and outside third-parties users. With the high profile fraud cases of the 1970’s and the numerous failings of savings and loans during the 1980’s, Wallace and White (p. 12) suggested that proposed legislation could well make reporting on internal controls mandatory. (Since that time, however, SAS 78 has superceded SAS 55 as
to the auditors understanding of the internal controls. No such legislation has been enacted that would mandate reporting on internal controls at the time of this writing.)

One of the hopes of mandatory reporting on a company’s internal controls as seen by Wallace and White, is a narrowing of the expectation gap for management and the internal audit committee. According to the authors,

"...a gap exists between the assurance explicitly conveyed and the expectations of management and audit committees. The expectation is that the internal auditing departments are performing sufficient auditing of internal control so as to provide the desired level of assurance. This is fueled by growing demands for public reporting by management as to the adequacy of design and the effectiveness of operations. Internal auditing practitioners who do not perform sufficient auditing in this regard, or who do not convey the desired level of assurance, or both, are apt to be found negligent should internal control difficulties arise. Public reports, reliance thereon, and associated implications have led to some liability considerations; however, both expectations and rules are changing nonetheless" (p. 12).

Wallace and White go on to explain that the internal auditor is in a “unique position to provide assurance to management and the audit committee as to the adequacy of design and effectiveness of the internal controls.” In fact, section 300 of the Standards for Professional Practice of Internal Auditing prescribes that the scope of the internal auditors work should encompass the examination and evaluation of the adequacy and effectiveness of the organizations internal control system.

A material weakness in the internal control process can be defined in part by considering whether routine operations would have detected the problem on a timely basis. If timely detection is deemed unlikely, the internal auditor needs to consider
whether the controls can be improved to ensure future timely detection. Other factors of a material weakness are its pervasiveness, and to what extent this weakness will impact the objectives of management. The auditor will also want to evaluate the corrective measures taken by management (p. 19).

In summary, as the business environment continues to experience changes to existing or the implementation of new technologies, the role of the internal auditor is changing. This change necessitates the internal auditor to adapt a new mindset and to expand his knowledge base and skill set in order to meet management’s expectations for audit reporting.

**Methodology**

Using an open-ended questionnaire, one member of the internal audit staff of six different companies was surveyed. Each was asked to respond from their experiences when new accounting software was implemented at their respective companies. Each company represented a separate industry or business, five of which are publicly traded corporations. Respondents were guaranteed anonymity to assist in obtaining full disclosure and accuracy.

The publicly traded companies include a soft drink bottler, a financial institution, a pharmaceutical manufacturer, a telecommunications company and an insurance company. The privately held company is a local retailer. Since these companies
were selected through personal contacts and willingness to participate, this was not a random selection. These companies varied widely in type. Therefore, the projection of these results to other companies may not be appropriate.

Each of the participants were senior internal audit personnel or higher. One of the publicly traded companies had no internal audit department. That function is outsourced to one of the big five accounting firms. The remaining publicly traded companies have at least 7 staff members in the internal audit department. The privately held company, however, had only one person, the CFO. He reports directly to the president of the company. Only three participants indicated their internal audit departments reports to an audit committee.

**Thesis Statement**

*When an entity implements a new accounting system or accounting software, the entity is at risk for error or material misstatement in general ledger and subsidiary accounts.*

If this statement is true, some effort must be expended to safeguard the assets of the entity. My goal was to determine what impact and procedural changes, if any, the internal audit department function would experience when a new system or accounting software is implemented.
Questions and responses

Major question: *What is the impact on the internal audit department function when an entity implements a new accounting system?*

The responses given addressed the function of the internal audit department and the implementation process separately. Implementation of a new system was considered a normal event in the course of business and not deemed as “impacting” in any unusual way the function of the Internal audit department. When their companies began planning for a new system or software, the majority saw their role as part of the design or development team. They evaluated and tested the controls before the new system was installed.

Subsidiary questions: *How does the internal audit department change its assessment of control risk when a new accounting system is implemented?*

*To what extent does the internal audit department change its assessment of control risk when a new accounting system is implemented?*

Each participant addressed these questions in different ways. Most often the responses indicated that any change could affect control risk. Significant changes such as implementing a new accounting system resulted in control risk being set at maximum with an increase in the testing and increased sample size.

1. *What are the effects on the daily routine of the internal audit staff when a new accounting system is implemented or what must the team do differently?*
While some of the respondents indicated that their function or daily routine was not affected, per se, some did describe what actually occurred in their departments. One important factor is the allocation of resources. Increased testing will require more time and possibly additional staff, depending on the knowledge base and skill set within the internal audit department.

2. **How much input did the internal audit department have, if any, in the selection and implementation of the new accounting system?**

Four of the six replies said that they had “little” input as to what system was actually selected, however, all of the participants said they were consulted in some way or actually participated in the development/installation process.

3. **If the new level of control risk is higher than the previous estimate, what method(s) is used in testing the internal controls?**

For those participants who were allowed to be part of the development process, the appropriate level of control risk was built-in or achieved before implementation. Other companies ran parallel systems or increased substantive testing, sample size or the scope of their post-implementation audit.

4. **Does a new system increase the level of control risk?**

Nearly all of the participants said no to this question. They indicated that because they participated in the design process or had an opportunity to test the new system prior to implementation, an acceptable level of control risk had already been built-in
or achieved. Their concern about control risk stemmed not from the actual system, but that of training for the new users.

5. *Are tests of controls increased when a new accounting system or accounting software is implemented?*

Overall, the participants said that test of controls increased. The difference was whether the internal audit department did testing during the design process or pre-implementation phase or post-implementation phase.

6. *What changes in testing are required in auditing an area with a new system?*

The responses indicated that changes in testing were not specifically required. The participants were more interested in the results of the testing. Concerns included the integrity of the processing and reporting of data, whether there are proper and effective controls are in place and adhered to, are errors reported and corrective action timely and was the testing relevant.

*What other information or comments would you like to add?*

One of the participants stated a need for adequate understanding of the new system prior to final selection. This was seen as valuable to management. Some companies have created technology teams to review systems and applications. These teams work with or are part of the internal audit department. One participant indicated that the internal audit department of his company has increased the number of CISA's due to the increased knowledge base required by the company.
Increased use of technology employed by their companies has required the internal audit department to become proactive and knowledgeable in reviewing new technology, forward thinking in its use and implementation, and more knowledgeable about technology in general.

Discussion and Analysis of the Responses

None of the participants took exception to the thesis statement. Two of the six overtly affirmed the thesis. One participant said that any change in an accounting system is an audit concern. In general, testing the controls of a new system is seen as a normal function of the internal audit department and implementing a new system had no unusual impact on the participants of the survey.

The internal audit departments from the survey made repeated mention of being proactive in the implementation of new accounting systems and software. While the majority of the participants indicated they had "little" input as to what system was actually selected, all of the participants were in some way consulted about their new system. Many were directly involved in the developmental process or played key roles in testing of the new systems prior to final selection and implementation. Yet, none of the participants of the survey mentioned a lack of independence when designing or consulting on the purchase of a new system. These internal auditors appear to have already assumed some of the characteristics of the "new" internal auditor previously discussed. Furthermore, these results seem to confirm the fact
that the internal audit department is increasingly called upon to act as consultants when new accounting systems are being considered.

Since any change in the technology of an entity, by definition, affects the level of risk assessment, training issues often accompany technological changes. If such changes are deemed insignificant, risk assessment need not be drastically increased. A new accounting systems or software, however, increased the level of control risk, if only at the beginning. Testing during development or post-implementation showed an increase in the test of controls, sample size and substantive tests for all of the survey participants. It is reasonable to assume that a company is implementing a new system because it is seen as an improvement over the old one. As seen in the survey results, the level of control risk may actually improve (decrease) once the new system has been tested and installed.

The daily routine of the internal audit department seemed unaffected by the implementation of new accounting systems or software. Testing in any form seemed a normal part of the internal audit function, and one with which they were all very familiar. Reallocation of resources would seem to be a critical factor whether it is for increased testing, training of existing personnel or hiring staff with a greater knowledge base or skill set.

Training of the users of the new system was another concern of the internal audit department. Much of the potential for error exists at the user level for any new
system. The training of personnel is a critical factor, not only in assessing control risk, but in the reliability of the data processed and the reports generated. While the internal auditor is not responsible for the actual training, often those technologically adept will participate in the training process. This seems to be a result of the increased skill set of the personnel being hired a members of or partners with the internal audit departments of today’s companies.

Finally, the internal audit departments were interested in the adequacy of the internal controls. Beyond the actual processes within the accounting system or software, are there adequate controls in place within the working environment? If there are controls in place, are they adhered to by management and other staff members? Is access restricted and are duties segregated? Are errors discovered and reported in a timely manner? The answers to all of these questions are part of the daily routine and ordinary function of the internal audit department.

Conclusions

None of the responses from the survey seemed outside the textbook parameters of a typical internal audit function. While each company will experience different needs at different times, and thus differ in their respective priorities, each of the participants provided appropriate responses to the questions they were asked. One factor that will affect the needs of a company is ownership (public vs. private). Another is it size. Smaller, privately held companies typically have less complicated audits or reporting requirements than larger, publicly owned companies. Considering such
differences, even the responses from the local retailer were reasonable. Such companies will often show more concern over smaller changes within their business. It is not uncommon for smaller companies to exhibit less segregation of duties. Furthermore, there may be no internal audit department or independent audit committee to report to in a privately held company.

Based on the responses from the participants and the information previously examined, the internal audit department is not unusually affected by the implementation of a new accounting system or accounting software. The audit professionals pursue customary audit methodologies to test the internal controls of the new systems and report to management their opinions of those controls. The internal auditors interviewed are actively participating in the implementation process within their respective companies and their participation is consistent with that described in the background information.

The participants of the survey agreed that the thesis statement was correct. The results, however, did not reveal that material errors or misstatements are actually occurring or that financial reports are misstated due to implementation of new accounting systems or changes to accounting software. The internal audit departments are performing their expected function and new systems are adequately tested before, during and after implementation.
Survey and Responses

Thesis Statement: *When an entity implements a new accounting system or accounting software, the entity is at risk for error or material misstatement in general ledger and subsidiary accounts.*

Soft drink bottler: This is a true statement....

Telecommunications company: True Statement. Any change in an accounting system is an audit concern.

Major question: *What is the impact on the internal audit department function when an entity implements a new accounting system?*

Insurance company: Our department attempts to be proactive in helping our organization manage risks associated with any critical systems implementation be it an accounting or operational system. To accomplish this we work with the systems design team and identify and communicate control design issues to the team as they are designing the system. For an accounting system design project, these issues typically include balancing controls, transaction edits and application security.

Financial institution: Other than audit’s involvement in ensuring proper controls are implemented with the system and proper project management practices and controls are used throughout the development and implementation process, the impact is nothing out of the ordinary.

Soft drink bottler: I'd say there is very little impact on the “traditional” internal audit department. I define the “traditional” internal audit role as a monitoring and reviewing capacity of company policy and procedures that are designed to safeguard the assets of the company. I believe they will be heavily reliant on the data that the new system produces, but will be hardly responsible for making sure the system works. The Internal Control Structure of a company has a whole LOT to do with how strong the policy is written and how closely the procedures are followed, but has little to do with the nature of the accounting package that is chosen.

The process of “implementing” a new, automated accounting package is very complex. It involves the skill sets of a variety of different people. Most companies implementing these packages do so using the services of an “ERP Implementation Consulting Company”. These consist of a highly specialized and talented group of individuals that know all there is to know
about the mechanics of the particular accounting package. They also must be very knowledgeable about business and accounting, enabling them to learn how the company operates pre-system, so they'll best know how to convert. Since these software packages are highly technical, but the application is highly “Accounting” oriented; you need to engage people who are adept at both. Usually, these consulting teams consist of two distinct types of people: a) those who know a LOT about the technical end (i.e. the code writers for the software, how the software was written and works, etc.) and a little about the accounting end, and b) those who are financial and accounting wizards (i.e. CPA’s), and know a little about the technical end. Together, they communicate the needs of the implementing group, and get the system up and running.

Another major concern with a new accounting system is the training aspect. You can’t just install a whole new integrated accounting package and expect people to just intuitively pick it up. It requires hundreds of hours of intense training. Without this, the risk of material misstatement increases dramatically. These consulting companies almost always assume the role of “trainer” as well, since they have done this more than anyone else.

Clearly, these are “requirements” that are beyond the scope of the “traditional” internal audit department. The “traditional” internal audit department will still need to go out and do field audits, interviewing employees and their job roles, documenting process flows, making sure the necessary Internal Controls are in place (i.e. Segregation of duties, Checks and Balances, Documentation, etc.). These things must exist regardless of the type of accounting package being used. Therefore, the “Role” of the traditional Internal auditor will not change.

These days, a new type of auditor has emerged onto the scene. Many larger companies are requiring the services and expertise of what are known as EDP auditors. These folks have been trained in a technical environment, and know how to analyze systems for “holes”. They have a keen understanding of the technical side, as well as a solid background in Internal Control analysis. These folks are experts in both the technical side and the accounting / control side. Their main role is to continuously “audit” the systems in place, making sure they are airtight. This includes making sure all Ledgers Balance with Sub-ledgers, all “Interface” portals are well-connected so that everything is being accounted for, and generally making sure the systems are functioning as designed. These people provide the assurance that the resultant data is credible, and that they system has integrity. These are the folks that bear the bulk of the burden upon implementation of a new accounting package.

Local retailer: The impact on the internal audit department function when a new accounting system is implemented is to increase test of controls and transactions.
Telecommunications company: None. The function or duties of the internal audit department do not change. Maintaining a continuous "audit" of the systems already in place is a function of the internal audit department.

Subsidiary questions:

How does the internal audit department change its assessment of control risk when a new accounting system is implemented?

Insurance company: Any significant change would typically drive an assessment of increased control risk. This assessment, of course, would be dependent on factors such as the scope/functionality of the new system, conversion schedule and materiality of the related processes/reporting.

Financial institution: The methodology we use to assess risk (inherent or control) would not change. Since we would probably be involved during the upgrade or replacement project, the control risk for the accounting function may change or may not change. It would depend on the results of our review during the project and the results of previous audits of that business area.

Soft drink bottler: Control Risk is the likelihood that a company's Internal Controls will fail to identify a material misstatement. Internal Controls generally fall into 5 broad categories that I touched on above... they are:
1. Segregation of Duties
2. Proper procedures for Authorization
3. Adequate Documents and record keeping
4. Physical Control over Assets
5. Independent Checks on Performance

To some degree, a new accounting package may "Strengthen" some of these controls. For example, by use of passwords and login's, only certain folks will be allowed to engage is specific transactions. This could strengthen the segregation of duties control because only authorized folks that do not violate the "conflict of interest" would be allowed to engage. To the extent that the new accounting package addresses these areas, the "traditional" internal auditor can place less emphasis on analyzing and testing for these controls.

Local retailer: We decided to increase our assessment of control risk to maximum and perform more substantive testing. Along with this, we would simultaneously test controls for these transactions.

Telecommunications company: For our in-house system, the first concern is the ability to change the operating program and the custody or protection of
the source codes. These codes need to be secured in order to protect the integrity of the system. Also, internal audit wants to make certain that all changes and modifications to programs are documented, reviewed, and approved; as well as sufficiency of back-up maintenance and contingency plans in case of system break-downs. Then the internal auditor looks into the adequacy and timeliness of training for the prospective users.

To what extent does the internal audit department change its assessment of control risk when a new accounting system is implemented?

Financial institution: A new system, by itself, could have minimal impact on the risk assessment. We would consider several other factors, as well as there being a new system, when assessing inherent and control risks.

1. What are the effects on the daily routine of the internal audit staff when a new accounting system is implemented or what must the team do differently?

   Insurance company: We would typically allocate additional resources to assess the control design of the new system as it is designed. This could involve significant resources depending on the new implementation.

   Pharmaceutical manufacturer: A new accounting system generally requires the audit staff be trained in the control features, how to use the system, and should the team use CAATS it requires changes to their software.

   Financial institution: None. Our concern is with the areas of the business that rely on that data and how they react. But it would have no effect on our day-to-day function.

   Soft drink bottler: Not much. Once the benefits of the new accounting package have been identified, and the audit control procedures have been modified accordingly, the internal auditors job is still to test the Internal Control structure of the locations in the field. The reliance placed on the numbers is already set due to the testings of the ERP Implementation teams and the EDP auditors, so “Data Integrity Testing” will not be applicable.

   Local retailer: The effects on the daily routine of the internal audit staff is two fold; one to ensure there are adequate controls in place with the new system and to test these controls. This will involve more time in the beginning of the new system.

   Telecommunications company: Any change in an accounting system is an audit concern. We would need to evaluate the internal controls of the system.
2. How much input did the internal audit department have, if any, in the selection and implementation of the new accounting system?

Insurance company: Typically our department has little input into the actual selection. We would have reviewed "request for proposal" documents to see if relevant criteria are included in the decision-making process.

Pharmaceutical manufacturer: Generally the internal audit departments have little say in the selection of new accounting systems. Forward thinking organizations however, solicit internal audit's opinion on control features, such as security, audit trails, etc. before purchasing a specific system. But controls are not always the primary consideration for buying a system â€” if this were so ERP systems like PeopleSoft would not have the customer base it has today.

Financial institution: Audit would concur on changes to controls within any business area.

Soft drink bottler: Not much. It was more the functional members... The real users of the product such as the managers, the financial accountants of the divisions, etc.

Local retailer: The internal audit/accounting department was an integral part in the selection of the new accounting system.

Telecommunications company: With our in-house accounting system, I was involved in strategic key points of the system development cycle. Internal audit involvement is advisable to ensure that the appropriate and adequate controls are built into the system. The internal audit department was also assisted by external CISA's.

With packaged accounting software, internal audit's main concern is the ability to change the operating program and the custodian (or protection) of the source codes. These codes are supposed to be secured by the software vendor.

3. If the new level of control risk is higher than the previous estimate, what method(s) is used in testing the internal controls?

Insurance company: As noted above, we perform a control design review to help ensure appropriate controls are designed into the new system and we would also on critical systems perform a "post-implementation audit" to
assess how effectively the controls designed into the system were actually working upon implementation.

Pharmaceutical manufacturer: More substantive testing is used as a matter of course. But it would depend on what the incremental risks are. For example, if the new system lacks integrity controls then more testing of balances.

Financial institution: We would use the same methodology we always use. We may adjust the sample size or review revised or new controls but our auditing methodology would not change. The scope of our audits could change.

Soft drink bottler: Most often, companies run “parallel” testing for long enough to be convinced there are no major “Disconnects”.

Local retailer: A new system increases the level of control risk because procedures may differ from the previous system. These procedures need to be updated and examined to ensure they fit within the present system and they are being applied. We will test the controls and transactions on a sample basis.

Telecommunications company: We increase our sample size and our substantive testing.

4. Does a new system increase the level of control risk?

Insurance company: Once stabilized a new system typically reduces control risk, through improved balancing, edits...it may have created. However, during the initial implementation period control risk is typically higher due to several factors including learning the new system, inadequate testing...

Pharmaceutical manufacturer: I don’t believe that the presence of a new system per se increases risk. The new system may provide superior controls to the system it replaces. On the other hand, as a systems auditor, I would rate the risk marginally higher with a new system that I had not had the ability to review before its implementation because its control features would be unknown to me. As a result, I more apt to put the system on my audit plan.

Financial institution: If proper development and change methodology is used, a new system by itself would not necessarily increase the level of control risk. However, administrative changes made to utilize the new software or system may increase the level of control risk.
Soft drink bottler: No. I think if it impacts it at all, it decreases it slightly.

Local retailer: Control Risk is increased when a new accounting system is implemented because the controls might change with the system and you want to ensure they are being followed.

Telecommunications company: Our internal audit department was present during the developing stages of our in-house system. The internal controls that were built into the system allowed us to set the control risk below maximum.

5. Are tests of controls increased when a new accounting system or accounting software is implemented?

Insurance company: For a significant new system testing of critical controls is typically increased.

Pharmaceutical manufacturer: Yes - Even if internal audit is involved in the development and rollout process. New control processes both within and outside of the systems need to be confirmed that they've rolled -out as management intended and are functioning day-to-day.

Financial institution: Not necessarily, though they could be. There are many other factors than just the software being used that would determine the level of testing done during a specific audit.

Soft drink bottler: Only upon implementation, to ensure everything is working as designed. After that, only the EDP auditors should be getting involved from a system perspective.

Local retailer: Test of controls are increased due to the inherent changes taking place and the possibility of different control procedures for the new system. Because of this, testing needs to increase, at least initially.

Telecommunications company: Our department was able to participate in testing the control features of the new system before it was fully implemented. One installed, tests of controls did not increase.

6. What changes in testing are required in auditing an area with a new system?

Insurance company: We have very little if any "required" testing of new systems. Our risk assessment typically would identify this as important work.
Pharmaceutical manufacturer: From the systems perspective, we'll look more carefully at the internal processing integrity, edit error correction, security, reporting accuracy, and interfaces to other systems. Areas that we would focus is on the software problem logs to see what problems are being experienced and whether the software support folks are correcting the problems timely. Also the potential impact of the problem to see if critical processing errors are being worked as a priority and to understand the impact to the financial statements if any. Where controls reside in the work flow more emphasis is placed on assuring that such controls are adhered to and whether the processes implemented can be made more efficient.

Financial institution: Possibly none. Possibly a broader scope could be required or more detailed testing or a review of revised or new processes and procedures.

Soft drink bottler: None. Since the data is assumed the same, the same tests used to assess the strength of the Internal Control from before will still be useful.

Local retailer: The changes in testing an area start with an understanding as it relates to the new system and apply appropriate tests.

Telecommunications company: Changes in testing are not as important as the knowledge base of the internal auditor of the new system. Our company has increased the number of CISA's in our company for this very reason.

What other information or comments would you like to add?

Insurance company: In a technology dependent company like Insurance company Insurance Co., effectively auditing new systems is very critical to providing timely information of value to Management.

Pharmaceutical manufacturer: Internal audit is not solely concerned with accounting systems. We generally want to be looking proactively at system controls for any new application that is critical to processing business in the company. This means that in our company's case - new manufacturing, e-commerce, warehousing and supply chain applications, payroll/personnel systems, etc. We get involved to help the project teams understand risk, assure that system and operational controls will be in place at go-live.

Financial institution: Within our organization, we have an Information Technology Audit Group that focuses only on new systems/applications and major system/application changes. They utilize a risk assessment methodology to determine which projects they will review and to determine
the extent of their involvement in the project review. By using a risk assessment for all new applications and systems in our organization, audit is able to be involved throughout the development, testing and implementation process. For a new financial system, we would use this means to ensure that adequate client/user testing done to provide adequate assurance that all financial processing is being properly accomplished. Being involved during the project phases also lets us evaluate the impact of the system on the business area and gain an understanding of the application ourselves and how it will be used by the business area. This process permits us to better evaluate the impact of new systems on the inherent and controls risk of the organization.

Retailer: None.

Telecommunications company: None.

General Demographics:

What is your title in the company?

Insurance company: Sr. Mgr. – Financial Audit

Pharmaceutical manufacturer: Director, Corporate Information Systems Audit

Financial institution: Vice President

Soft drink bottler: Corporate Accounting Manager

Local retailer: Chief Financial Officer

Telecommunications company: Senior Internal Auditor

How many people are on the audit staff?

Insurance company: 60-65

Pharmaceutical manufacturer: 14

Financial institution: 16

Soft drink bottler: None. We outsource all of that to a big five firm.
Local retailer: 1, I am the accounting/auditing department

Telecommunications company: 7

To whom does the internal auditor report at your company?

Insurance company: Chief Financial Officer

Pharmaceutical manufacturer: CFO

Financial institution: CFO for administrative purposes, Audit committee of the BOD for functional purposes

Soft drink bottler: The auditors report back to the Audit Committee of the Board of Directors.

Local retailer: The president of the company

Telecommunications company: The CFO and Audit Committee

What is the size of the company?

Insurance company: $27 Billion in annual revenue, $98 Billion in assets, 50,000 employees.

Pharmaceutical manufacturer: $6.4 Billion in annual revenues, $9.6 Billion in assets, 41,000 staff and 175 locations.

Financial institution: $622 Billion annual revenues, $28 Billion in assets.

Soft drink bottler: $2.2 Billion in annual revenues, $2.9 Billion in assets.

Local retailer: $3.5 Million in annual revenues, $1.6 Million in assets. Telecommunications company: Recently merged, consolidated financial statements not yet available. $58.5 Billion in combined annual revenues, $113.4 Billion in combined assets.
References

Consideration of the internal control structure in a financial statement audit.
Jersey City: American Institute of Certified Public Accountants.

Amendment to statements on auditing standards to recognize the internal control-integrated framework report.
Jersey City: American Institute of Certified Public Accountants.


The Institute of Internal Auditors. (1997.) *Standards for the professional practice of internal auditing.* Altamonte Springs: The Institute of Internal Auditors Research Foundation.
