Audit Risk Attributes In Computerized Environments

Timothy B. Bell, (tbell@kpmg.com), KPMG Peat Marwick, Montvale, NJ

W. Robert Knechel, (knechewr@dale.cba.ufl.edu), University of Florida

Jeff L. Payne, (jpayne@olemiss.edu), University of Mississippi

Abstract

This study examines the relationship between important risk attributes of computerized accounting systems and the errors generated by those systems. The incidence and magnitude of errors are measured using misstatements detected by external auditors. We provide evidence that account classification, company size, information technology (IT) complexity, and the extent of IT within the accounting information system differentially affect the incidence of IT-related misstatements. Overall, these results indicate that the increased control facilitated by use of IT is not universal but that IT provides many benefits that should be considered by external auditors during the planning of an audit engagement.

Introduction

The application of information technology (IT) to accounting information systems (AIS) creates opportunities for increased control (i.e., echo checks, validity checks, edit checks, sign checks, and range checks) and enhanced productivity. However, IT exposes accounting information systems to significant new risks (i.e., hardware failure, software development, and unauthorized access). The empirical connection between these concerns and the risks of misstatements being included in account balances is incomplete. Bell *et al.* (1998) compared computerized and noncomputerized accounting information systems to assess the differential impact of computerization on common attributes of accounting errors (e.g., faulty identification and processing of transactions). They found that the recording of exchange documents, incorrect application of in-

ternal controls, and inadequate internal controls were more likely to be sources of problems when information systems were computerized than when they were not.

This study extends Bell *et al.* (1998) by focusing on risk attributes that are specifically relevant to *computerized* accounting information systems. We adopt a view of system reliability that would be appropriate for an external auditor engaged to examine an organization's financial statements. Consequently, we use audit differences (auditor detected misstatements) as our measure of system reliability. Audit differences are defined to include accounting errors (unintentional misstatements) and fraud (intentional misstatements). We then investigate the differential effects of risks associated with computerized systems on the generation of accounting errors across account classification, company size, accounting information system complexity, and the extent of IT utilization within the accounting

Readers with comments or questions are encouraged to contact the authors via e-mail.

information system.

A detailed questionnaire was developed to gather information on the relationship between computerized AIS attributes and the incidence of audit differences. This survey was distributed to a randomly selected sample of audits from an international accounting firm. Part I of the survey requested general engagement information such as audit gauge (a measure of materiality), extent of system computerization, and AIS complexity. In Part II, respondents were asked to identify audit differences detected in the course of the engagement and provide an assessment of a number of attributes for each error, including the error's relation to computerized processing.

Our examination of risk attributes by account classification reveals that inventory has the most errors attributed to the client's computer system while computer system-related errors are largest in accounts payable and accruals. Analysis by company size indicates that small companies have problems implementing microcomputer and end-user applications and properly handling exception reports; moderate size companies have difficulties with improper computer processing; and large companies have problems with IT personnel, internally developed software and improper computer processing. Complex accounting information systems are affected by problems with IT personnel, incorrect program changes, and improper computer processing. These risk areas are also responsible for the largest errors. Accounting information systems that are partially automated have the most errors due to improper implementation of microcomputer and end-user applications and incorrect program changes. Furthermore, IT-related errors are also larger for partially computerized accounting information systems. Overall, IT-related errors are not pervasive. When these errors do occur, they can have a significant effect on reported financial statement balances, however.

The remainder of the paper is organized

as follows. The next section describes the risk assessment for computerized AIS. The second section discusses the relationship among accounting errors, controls and audit differences. The third section raises the specific research questions to be addressed in the study. The fourth section describes the approach to data gathering. The results of the empirical analysis are presented in section five. Limitations are discussed in section six. A summary and discussion is presented in section seven and suggestions for future research are contained in the last section.

Risk Assessment for Computerized Accounting Information Systems

A computerized AIS environment consists of two types of internal controls: application controls and general controls. *Application controls* are designed to prevent, detect and correct errors and fraud in individual transactions as they are processed within the system. *General controls* are designed to assure that application controls operate in the most effective manner.

Application controls can be applied to input, processing or output. *Input controls* are designed to assure that information initially captured within the system is accurate, complete and properly authorized. A key concern of input controls is the transformation of information to electronic form. *Processing controls* are designed to assure that transactions in the system are manipulated correctly and appropriately. These controls ensure that computations, aggregations and postings are accurately performed. Finally, *output controls* provide assurance that the output from the system is appropriately reported for an effective and efficient response.

General controls are broader in nature and are designed to provide assurance that transaction processing occurs in a properly controlled and consistent manner. Some of the concerns of general controls include system development and maintenance, system security and access, data-

base integrity, reliability of end-user computing and contingency planning.

Information technology is rapidly being embedded in an increasingly larger portion of business and information processes, as well as across such processes. This increases the need to explicitly consider information technology when assessing the effectiveness of an organization's internal control. Auditors need the ability to understand, identify, suggest, implement, and evaluate controls in today's IT-based organizations (Hollander *et al.* 1996). Additionally, new audit methodologies are increasingly emphasizing the role of management and process controls in audit planning (Knechel 1998). In spite of these recent trends, auditors have historically relied on special experts to assess the reliability of computerized AIS. As a natural outgrowth of this philosophy, many auditors feel they lack the expertise to adequately evaluate and test automated systems.

As accounting systems increasingly utilize IT, auditors need to consider the opportunities for increased control that are not available in a manual system. The computer's ability to scan all transactions, perform edit and field checks, and compare and reconcile data across systems and sources can be used to greatly improve the reliability of information processing. Unfortunately, many auditors fail to recognize these beneficial capabilities and do not adequately factor the existence of such controls into their assessment of AIS. The appropriateness of such a strategy needs to be reconsidered in light of current trends. For example, Statement on Auditing Standards No. 80 (effective date January 1, 1997) emphasizes the relationship between IT and audit planning: "In entities where significant information is transmitted, processed, maintained, or accessed electronically, the auditor may determine that it is not practical or possible to reduce detection risk to an acceptable level by performing substantive tests for one or more financial statement assertions. In such circumstances, the auditor should perform tests of

control to gather evidential matter to use in assessing control risk, or consider the effect on his or her report." (AICPA 1997, AU 326, ¶14). In order to adopt appropriate strategies and better understand the influence of computerization on accounting information systems, auditors need a more complete understanding of the relationship between system attributes (especially IT-related controls) and processing errors.

Relationship among Errors, Controls and Audit Differences

In this paper we adopt a view of system reliability that is appropriate for an external auditor. Consequently, we focus on audit differences that are detected during the course of an examination of financial statements. Audit differences are defined to include accounting errors and fraud. We do not examine the extent of all processing errors within an information system, only those that are related to the financial statements and that are significant (material) to the financial results of the company. Of course, there can be many other errors that occur within an information system but our data does not allow us to address small or nonaccounting errors. A great deal of understanding about audit differences has been obtained as a result of existing research, particularly as relates to the size, frequency and distribution of audit differences across account areas; the causes of audit differences; the audit procedures that are most effective at signaling audit differences; and the relationship between environmental characteristics (such as internal control) and the incidence and magnitude of audit differences. A discussion of this literature can be found in Bell *et al.* (1998).

In order for an auditor to detect an audit difference, a number of events must occur. The sequence of events linking an accounting error to an audit difference are depicted in Figure 1. Every organization manifests a control environment. This affects the likelihood that an error will occur within a system. The control environment includes any controls that are specifi-

cally designed to prevent errors from occurring, many of which will be built into computerized information systems. However, once an error has occurred, it will also be subject to detective and corrective controls which may remove the processing error from the system. Detective controls are often technology-based but corrective controls usually require human intervention. Finally, if the error remains undetected by the system, it may still be detected by the auditor during the course of the audit. Auditor-detected errors are considered to be audit differences and provide the data for our study.

This perspective does not allow consideration of errors that are prevented or corrected by internal controls, nor does it incorporate any errors that remain undetected by the auditor. However, since the auditor's risk concerns only arise after the system has completed its operations, errors removed by detective and corrective internal controls are not the responsibility of the auditor. In fact, the auditor's testing procedures

are conditional on the assessed level of error which is expected to escape undetected by the control system (AICPA 1997, AU 312). Regarding errors that are undetected by controls *and* the auditor, unless such audit failures are systematic and endemic to common audit approaches, the general assumption is that such errors will be small and/or randomly distributed. As a result, we feel it is appropriate to use data concerning detected audit differences to assess system reliability from the viewpoint of the external auditor.

Statement of Research Questions

The Attributes of IT-Based Audit Differences

We examine the relationship between common risks in computerized AIS and the frequency of audit differences. Given the dearth of empirical evidence relating the incidence of audit differences to the presence or absence of IT related controls, we gathered data on the application and general control attributes of audit differences. The specific risks we address in this paper were derived from numerous professional sources such as professional standards, practitioner-oriented training material and textbooks.

Two sources are extremely useful for identifying risks associated with computerized AIS: *Systems Auditability and Control* (SAC) (1992) by the Institute of Internal Auditors and *Internal Control: An Integrated Framework* (COSO) (1992) by the AICPA. SAC included an empirical examination of perceived risks related to computerized AIS. Overall, the two risks cited most frequently in the SAC Report were "unauthorized access or changes to data and systems" and "data accuracy and integrity". Both of these risks could impact accounting information. Another accounting-related risk that was mentioned was the "lack of available skilled human resources". In the following discussion of our research questions, we have provided references to relevant professional literature where possible.

Risks Associated with General Controls

As previously discussed, general controls are used to assure that the computer system is operating as designed and is not changed in an unauthorized manner. Many general controls deal with the proper roles of IT personnel and interactions with personnel external to the information system. SAC (1992, pp. 9.4 – 9.5) has a discussion of specific risks arising from people interacting with IT, including human error, dishonest employees, outside intervention, physical damage and computer viruses. Additionally, general controls deal with system security and documentation of authorized procedures. We look at specific general control attributes that may be associated with IT-related audit differences as included in the following propositions:

- P1 Overworked IT personnel will be associated with AIS-related audit differences.
- P2 Incompetent IT personnel will be associated with AIS-related audit differences.
- P3 Poor segregation of duties among IT personnel will be associated with AIS-related audit differences.
- P4 Poor segregation of duties between IT personnel and information users will be associated with AIS-related audit differences.
- P5 Poor system documentation will be associated with AIS-related audit differences.
- P6 Inadequate access controls will be associated with AIS-related audit differences.
- P7 Hardware failure will be associated with AIS-related audit differences.

General controls also apply to system development. Risks associated with different sources of software are discussed extensively in SAC (1992 pp. 5.64 – 5.75). General risks across multiple system platforms (other than traditional mainframe processing) include reduced access security, unreliable system development, improper program changes, lack of data consistency, lack of documentation, poor contingency and recovery planning, and copyright violations.

Specific risks are associated with microcomputers, networks, workstations, operating systems, database software, fourth generation languages, spreadsheets and decision support systems. End user computing has two further specific risks to be considered: (1) risks associated with microcomputers including inadequate physical and logical access controls, unrestricted remote access and unknown copies or different generations of sensitive data and (2) risks associated with spreadsheets including excessive complexity, use of incorrect assumptions or calculations, inaccurate data entry, poor labeling, uncontrolled modification, erroneous or accidental replacement of cell formulas or data, unreliable migration to new applications, unreliable macros and inadequate testing.

Obviously, a system that is improperly designed, programmed or implemented may generate unreliable results. Since system software and applications may come from different sources (e.g., external vs. internal development) and get used at different levels of the organization (e.g., centralized vs. distributed vs. desktop processing), we expect the risks of each will vary. Furthermore, to the extent that personnel within an organization have the ability to modify program code, problems can be caused by improper or incorrect changes to otherwise reliable systems. We expect numerous system development attributes to be associated with AIS-related audit differences as reflected in the following propositions:

- P8 Problems with the implementation of purchased software will be associated with AIS-related audit differences.
- P9 Problems with the implementation of internally developed software will be associated with AIS-related audit differences.
- P10 Problems with the implementation of microcomputer applications will be associated with AIS-related audit differences.
- P11 Problems with end-user applications will be associated with AIS-related audit differences.

- P12 Inadequate/improper design specification will be associated with AIS-related audit differences.
- P13 Incorrect program coding will be associated with AIS-related audit differences.
- P14 Improper/incorrect program changes will be associated with AIS-related audit differences.

Risks Associated with Application Controls

We also consider risks arising from application processing. This covers the sequence of events that starts with data entry and corresponds to the actual manipulation and reporting of individual transaction data. Application controls are used to increase the reliability of processing. Data entry is considered to be a common source of mistakes because it may involve transformation of data into electronic form (e.g., keying or scanning of data). Breakdowns in subsequent processing can be caused by hardware or software problems, improper processing by human agents or improper handling of exceptions. We propose that the following application processing concerns will be associated with AIS-related audit differences:

- P15 Data entry errors will be associated with AIS-related audit differences.
- P16 Improper computer processing will be associated with AIS-related audit differences.
- P17 Improper/incorrect handling of exception reports will be associated with AIS-related audit differences.
- P18 Incorrect program used in processing will be associated with AIS-related audit differences.

Impact of Specific Conditions on Risk Attributes

Based on prior general research dealing with audit differences, we expect that a number of characteristics are likely to affect the impact of the above attributes on the incidence and magnitude of AIS-related audit differences. The

primary purpose of this study is to examine the differential effects of the following system characteristics on the specific risk attributes:

Type of account: Different accounts in the financial statements are subject to different degrees of computerization. Accounts such as fixed assets may be comprised mostly of routine transactions that are amenable to effective computerization. Other accounts, such as receivables that are subject to control risk related to cash receipts and valuation issues, may consist of a larger proportion of nonroutine transactions and would thus be less effectively controlled through computerization.

Company size: Larger companies generally have more complex information systems and rely more on IT to foster timely and reliable information processing. However, larger organizations may also be more difficult to logistically link and may require the use of more complex IT architectures. The availability of competent IT personnel is also potentially related to the size of an organization.

AIS complexity: The effectiveness of controls regarding the use, development and application of AIS could be affected by the complexity of IT used within accounting applications. Complex systems require high user dependence on IT control procedures. Characteristics of complex systems can include professional programming and operating capabilities and the presence of large multi-user computer systems. These complex systems may tend to rely more on internally developed or customized software applications. Less complex systems can be based on a PC platform and use "canned" software with little or no modification.

Extent of mixed manual/computerized processing: The completeness of computerization can also affect the reliability of AIS. Systems that are based on a seamless linking of IT applications (e.g., SAP or Oracle based systems) may be less susceptible to processing failures; proc-

essing errors could occur more frequently when systems are partially automated due to confusion regarding proper procedures and manual linkages between systems that are subject to error.

Survey Method

The sample investigated was based on the availability of data and other research considerations. The data used for this study was collected using the same survey instrument used for Bell *et al.* (1998). For each audit difference identified, the survey respondent was required to answer a series of questions dealing with attributes of the audit difference. One series of attributes dealing with traditional control classifications (e.g., incorrect manual computations) were examined in Bell *et al.* (1998). This study focuses on additional risk attributes that are relevant to computerized AIS only.

In the survey general engagement information such as audit gauge (the dollar value used for planning materiality), extent of system computerization, system complexity, and whether reliance was placed on automated and/or user controls was requested. Next, respondents identified audit differences detected in the course of the engagement and answered a series of questions for each audit difference. Audit differences include accounting errors (unintentional misstatements) and fraud (intentional misstatements). Immaterial audit differences were included, but not entries at the request of the client

(e.g., tax provision entries). The questions for each audit difference were derived from a detailed examination of general and application controls. Due to the comprehensive nature of the survey, some of the IT attributes of audit differences had to be assessed in general terms. Questions could not address all specific error causes in detail so some were attributed to "processing" in general.

After pretesting the survey instrument on a small number of engagements, surveys were mailed directly to respondents. The survey was completed by either the manager or senior on the engagement and reviewed by the computer audit specialists that were used on each specific engagement.

A target sample was randomly selected from a large international accounting firm's U.S. client database. The target population (a random sample of 385 audit engagements for fiscal 1988) includes both public and private entities (including not-for-profit entities). Responses were received for 358 engagements. Seventy-nine responses were eliminated for accounting information systems that were not computerized. An additional 116 responses were eliminated because they were not full scope audits (82) or audits of financial institutions (34), yielding a final sample of 163 full scope audit engagements. Respondents indicated that the survey instrument took approximately 6 hours to complete.

Table 1
Classification of Survey Engagements by Industry

Industry	Surveys		Audit Differences	
	Number	% of Total	Number	% of Total
Agriculture	10	6.1	61	6.8
High Technology	10	6.1	66	7.4
Manufacturing	50	30.7	315	35.3
Merchandising	35	21.5	201	22.5
Real Estate	9	5.5	25	2.8
Other	49	30.1	225	25.2
Totals	163	100.0	893	100.0

Table 1 reports the industry composition of the final sample of 163 engagements and 893 audit differences. On average, 5.60% (11.42%) of the audit differences were larger than gauge (50% of gauge) and 4.80% of the audit differences were considered to be fraud.

Bell *et al.* (1998) reported a few general results related to the incidence of IT-related audit differences. Of the 893 audit differences analyzed in their study, only 8.40% were due to breakdowns or failures related to IT. Their overall results are summarized in Table 2 for AIS-related audit differences. They found that data entry errors were the most common source of AIS-related misstatements (62.86% of audit differences detected were affected by data entry problems). Problems with general controls, other than development controls, result most often from incompetent IT personnel (13.21%) while inadequate access controls did not lead to any reported audit differences in their sample. As a group, problems with system development were also a frequent source of misstatements.

Results

Extending the analysis of Bell *et al.* (1998), we examine audit differences for a number of IT characteristics that may affect the risk attributes of accounting information systems. Our results are presented in this section based on the previously discussed research questions.

Analysis by Account Group

The AIS-related misstatements were evaluated across account groups. The average number of AIS-related misstatements is significantly different across account groups ranging from a high of 13.97% (of total audit differences for the account) for inventory down to 2.86% for other current assets and 3.51% for receivables ($p < .05$, Chi-square test of audit difference frequencies across accounts).

Looking at individual account groups

we can see that there are different patterns of IT-related error attributes for each group. These are summarized as follows:

Accounts Receivable: AIS-related audit differences arose due to errors in processing with improper handling of exception reports (100.00%) being the most frequent followed by improper processing (56.98%) and data entry errors (56.84%). The magnitude of these audit differences hovers around 1%, however, indicating that they are not economically significant.

Inventory: Inventory reveals a broad spectrum of problems related to IT controls. Overall, the most frequent source of misstatement is data entry errors (58.97%) while microcomputer software (20.51%) and improper program testing (17.95%) rank second and third, respectively. Looking at magnitudes, however, we only see significant magnitudes for differences attributable to the automation of the client's computer system (18.72%), data entry errors (10.13%), and implementation of purchased software (5.50%). Incompetent IT personnel are the most common source of problems within general controls (12.82%, $p < .05$, significance determined using the Kruskal-Wallis (KW) test for audit difference frequency between the respective error causes within control classification). Misstatements are also frequently due to IT development. However, none of the error causes creates significantly more audit differences than the group as a whole. Data entry errors are the most common source of errors within application controls.

Other Current Assets: There were very few audit differences observed in other current assets and these were all attributable to data entry errors, improper use of exception reports and implementation of user developed spreadsheets.

Fixed Assets: AIS-related audit differences in the area of fixed assets generally arise from data entry errors (68.86%) or development problems related to internally developed software

Table 2
Summary of Aggregate Audit Difference Rates and Magnitudes

		Audit Difference Rate (1)	Audit Difference Magnitude (2)
Total number of audit differences		893	893
Total number of complete surveys		163	163
Average number of audit differences per engagement		5.479	5.479
	Was the difference attributable to the client's computer system?	** 8.40	** 24.93
General Controls			
P1	Did the difference occur because of overworked IT personnel?	3.33	40.00
P2	Did the difference occur because of incompetent IT personnel?	** 13.21	* 58.50
P3	Did the difference occur because of poor segregation among IT personnel?	1.67	26.00
P4	Did the difference occur because of poor IT personnel/information user segregation?	* 5.00	6.67
P5	Did the difference occur because of poor system documentation?	3.21	106.50
P6	Did the difference occur because of inadequate access controls?		
P7	Did the difference occur because of hardware failure?	1.55	54.00
General Controls - Development			
P8	Did the difference occur due to problems with the implementation of purchased software?	* 12.74	30.88
P9	Did the difference occur due to problems implementing internally developed software?	* 22.86	* 24.00
P10	Did the difference occur due to problems implementing microcomputer applications?	** 20.71	* 8.92
P11	Did the difference occur due to problems implementing end user applications?	** 22.86	* 27.29
P12	Did the difference occur due to inadequate/improper design specifications?		
P13	Did the difference occur due to incorrect program coding?	* 4.88	76.67
P14	Did the difference occur due to improper/incorrect program changes?	** 20.71	* 40.08
Application Controls			
P15	Did the difference occur due to data entry errors?	** 62.86	** 17.96
P16	Did the difference occur due to improper computer processing?	** 28.21	* 27.61
P17	Did the difference occur due to improper/incorrect handling of an exception report?	** 19.40	* 35.42
P18	Did the difference occur because of incorrect program used in processing?		

- (1) Audit difference rates represent the percentage of times the respective control attribute was identified as a cause of an audit difference. For example, an audit difference rate of 4% indicates that for all errors found, 4% were affected by this specific control attribute.
- (2) Audit difference magnitudes were calculated based on the percentage of gauge (dollar value of preliminary planning materiality) for the audit client. For example, an audit difference magnitude of 1% would indicate that the errors found were on average one percent of planning materiality. This percentage is calculated for control characteristics for which the survey response indicated the respective attribute contributed to the audit difference.

* Percentage is significantly different from zero at $p < .05$

** Percentage is significantly different from zero at $p < .01$

Significantly different ($p < .05$) based on the Kruskal-Wallis test of audit difference frequency between the respective error within control classification. For example P2 was greater than the other potential IT risk within general controls.

(55.87%), microcomputer software (53.83%) or user developed spreadsheets (54.62%). Significant error magnitudes are due to the client's computer system (21.50%) and data entry errors (19.50%).

Accounts Payable and Accruals: AIS-related audit differences in this account area exhibit a broad spectrum of AIS attributes. The most frequent source of problems under application controls are data entry errors (59.26%) followed by improper computer processing (29.63%). AIS-related audit differences also tend to be quite large for attributes related to the client's computer system (34.85%) and data entry errors (26.75%).

Although audit differences directly caused by the computerization of accounting information systems are few, there are patterns we can observe across accounts. When audit differences occur, they tend to be related either to system development or application controls (especially data entry). Consequently, these are the areas that should be the focus for assessing the control risks of a system. More specifically, given the broad spectrum of error attributes and the size of the audit differences related to inventory, fixed assets, and payables, auditors are well advised to be very careful when planning their examination of these areas in a computerized environment.

Analysis by Company Size

In order to analyze the relationship of size of company to the incidence of AIS-related misstatements, we split the sample into three different size categories (small/moderate/large) based on gauge. The larger the company, the more misstatements found in the sample (4.714 small / 5.750 moderate / 7.724 large, $p < .05$, Chi-square); but smaller companies appear more likely to have IT-related misstatements, as evidenced by an error frequency of 9.31% as compared to 7.73% for moderate companies and 7.14% for large companies. This result might

be expected because smaller companies are less likely to have the necessary expertise to run complex computerized systems—complex AIS were present in 29.00% of small, 28.99% of moderate, and 61.61% of large companies. On the other hand, larger companies are likely to be more extensively computerized and thus have more chance of having IT-related problems occur—totally automated AIS were present in 46.10% of small, 53.14% of moderate, and 83.04% of large companies. The most frequent cause of IT-related problems for all companies is data entry (58.14%, 68.75%, and 56.25%, respectively). Moderate and large companies also have frequent problems associated with improper processing (31.25%/50.00%). Problems of overworked IT personnel are more likely for moderate companies but no such problems were observed in the small and large categories. We see that hiring and training of IT personnel becomes a more frequent source of error as companies get larger, rising from 2.33% for small to companies to 12.50% for moderate companies and 31.25% for large companies. Neither of these results carry over to error magnitudes, however.

These results are interesting when considered jointly because they seem to indicate that small companies may not have problems with IT personnel because they are too small to hire such specialists (possibly relying on outsourcing of some type) as indicated by the low levels of internally developed software, while moderate companies begin to build an AIS department but have problems with understaffing. Finally, large companies make the commitment to adequate staffing but have trouble with the overall caliber of IT personnel and the complexity of applications which is also evidenced by the errors due to internally developed software.

Analysis by Extent of Computerization

To analyze the effect of the extent of computerization on the incidence of audit differences, we split the sample into two different

classifications, partial and total (survey responses available were total, partial, or no computerization). Audit differences occur more often in totally computerized environments (6.610 total vs. 4.465 partial, $p < .05$, Chi-square), but the influence of the client's computer system on the generation of audit differences is not affected by the overall level of computerization. Partially computerized accounting information systems appear to have more development problems; totally computerized AIS problems exhibit more frequent problems with internally developed software and end user applications. Data entry errors are a significant cause of audit differences irrespective of the level of computerization but the magnitude of errors is larger for partially computerized systems (32.58% vs. 18.58%). Overall, the level of computerization appears to influence the implementation of IT, but it is possible that the higher overall level of audit differences in totally computerized AIS may reflect the superior error detection capability of those information systems

Analysis by Complexity of AIS

To analyze the influence of the complexity of the AIS environment on the incidence of AIS-related audit differences, we split the sample into two different classifications, complex and not complex AIS (survey respondents classified information systems as complex or not complex). Audit differences occur more often in highly complex AIS (6.776 complex vs. 4.921 not complex, $p < .05$, Chi-square), but the complexity of the AIS does not influence the generation of audit differences. Focusing on complex systems we see that problems arise due to incompetent IT personnel (32.00%), improper/incorrect program changes (28.00%), data entry errors (48.00%), and improper processing (44.00%). These differences are all of significant magnitudes as well. Less complex environments have consistent problems with AIS development, especially in the implementation of microcomputer applications and end-user applications. With the exception of end-user applica-

tions, the size of errors in less complex AIS are relatively small.

In summary, the complexity of the AIS influences the ability to hire and retain competent IT personnel. This creates problems with internally developed applications, modification of existing applications, and the related processing of those applications. Less complex AIS are still in the process of designing and implementing microcomputer (PC based) applications and refining the input and output processing controls.

Limitations

Research using actual audit differences is limited to insights on discovered errors. Given the number of engagements and audit differences included in the analysis, we expect the sample to be fairly representative of discovered and undiscovered errors. Additionally, the data used in our analysis represents *ex post* judgments from the professionals on the respective audit team. A concern is that recollections concerning risks and the presence of selected attributes may be flawed due to cognitive limitations. The auditor's ability to review the extensive documentation supporting audit decisions made during audit engagements mitigates this concern.

Another potential limitation is the data's age. Obviously, IT has changed in the past few years but we do not feel that this limits the contribution of our results. The use and understanding of IT's impact on AIS has greatly improved, but our knowledge is still incomplete. Additionally, a significant portion of businesses, especially smaller ones, are still adopting, updating, and converting their AIS with new IT (McKenney 1995). One result from our study that could be influenced by the age of the data are problems associated with data entry. With the pervasive use of scanning technology it is possible that previously observed error rates associated with manual data entry will have declined dramatically.

Summary and Discussion

The concerns about information system risk that were identified in this study have generally received extensive discussion in the professional and educational literature and are familiar to most IT professionals, internal auditors and external auditors (Wallace 1991; Warren et al. 1998). A number of questions were asked as part of the motivation for this study. Specifically, we investigate the differential effects of information systems risks associated with computerized information systems on the generation of accounting errors across account classification, company size, accounting information system complexity, and the extent of IT utilization within the accounting information system. In spite of the limitations mentioned above, the data reported in the preceding sections provides partial answers to many of these questions.

Overall, IT-related audit differences are relatively rare, even in account areas that are heavily computerized. However, when these errors do occur, they can have a significant impact on reported balances. The most significant causes of IT-related audit differences were problems with data entry, internally-developed software (mainframe), microcomputer applications (including end-user computing applications), improper computer processing, improper/incorrect program coding, and problems with IT personnel. There were no audit differences that were due to unauthorized access or changes to systems or data.

The survey by the Institute of Internal Auditors, *Systems Auditability and Control* (1992), isolated "unauthorized access or changes to data and systems" and the "lack of available skilled human resources" as potential significant risks to AIS. Our results do not support the first observation but are supportive of the second. The studies differ in that this study is based on the analysis of errors detected in the course of actual audit examinations while SAC is based on general impressions of survey respondents. This

indicates a need to continue research in this area to test the robustness of the SAC report's findings and recommendations.

Suggestions for Future Research

Our evidence calls for continued research into the causes of error and effectiveness of IT controls within AIS. Information technology continues to increase productivity by reducing manual processes (e.g., Electronic Data Interchange (EDI), Electronic Funds Transfer (EFT)). The impact of IT on AIS is leading auditors such as Elliott (1997) to propose new assurance services that will focus on the non-financial components of the accounting information system. Additionally, the accounting profession is looking at new forms of financial reporting, some that can be based on interactive communication between the user and preparer of financial information. This rapidly changing environment requires that we continuously update our understanding of the effectiveness of IT controls within the AIS.

References

1. American Institute of Certified Public Accountants, *AICPA Professional Standards*, CCH Incorporated, Chicago, Ill., 1997.
2. Bell, Timothy B., W. Robert Knechel, Jeff L. Payne and John J. Willingham, "An Empirical Investigation of The Relationship Between the Computerization of Accounting Systems and The Incidence and Size of Audit Differences," *Auditing: A Journal of Practice and Theory*, Vol. 17, No. 1, pp. 13-38, 1998.
3. Committee of Sponsoring Organizations (COSO), *Internal Control: An Integrated Framework*, American Institute of Certified Public Accountants, Jersey City, New Jersey, 1992.
4. Elliott, Robert K., "Assurance Service Opportunities: Implications for Academia," *Accounting Horizons*, Vol. 11, No. 4, pp. 61-74, 1997.

5. Hollander, Anita. S., Eric L. Denna and J. Owen Cherrington, *Accounting, Information Technology, and Business Solutions*, Richard D. Irwin, Chicago, Illinois, 1996.
6. Institute of Internal Auditors, *System Audibility and Control*, Institute of Internal Auditors, Altamonte Springs, Florida, 1992.
7. Knechel, W. Robert, *Auditing: Text and Cases*, South-Western College Publishing, Cincinnati, Ohio, 1998.
8. McKenney, James L., *Waves of Change: Business Evolution Through Information Technology*, Harvard Business School Press, Boston, Massachusetts, 1995.
9. Wallace, Wanda A., *Handbook of Internal Accounting Controls*, Prentice Hall, Englewood Cliffs, New Jersey, 1991.
10. Warren, J. Donald Jr., Lynn W. Edelson, Xenia L. Parker, Rita M. Thrun, *Handbook of IT Auditing*, RIA Group/WG&L, Valhalla, New York, 1998.