Communications of the Association for Information Systems

Volume 27 Article 28

10-2010

Beyond Regulatory Compliance for Spreadsheet Controls: A Tutorial to Assist Practitioners and a Call for Research

Linda A. Leon
Loyola Marymount University, Linda.Leon@lmu.edu

Dolphy M. Abraham
Alliance Business School

Lawrence Kalbers
Loyola Marymount University

Recommended Citation

Leon, Linda A.; Abraham, Dolphy M.; and Kalbers, Lawrence (2010) "Beyond Regulatory Compliance for Spreadsheet Controls: A Tutorial to Assist Practitioners and a Call for Research," *Communications of the Association for Information Systems*: Vol. 27 , Article 28.
DOI: 10.17705/1CAIS.02728
Available at: https://aisel.aisnet.org/cais/vol27/iss1/28

Communications of the Association for Information Systems

CAIS

Beyond Regulatory Compliance for Spreadsheet Controls: A Tutorial to Assist Practitioners and a Call for Research

Linda A. Leon

Loyola Marymount University

Linda.Leon@lmu.edu

Dolphy M. Abraham

Alliance Business School

Lawrence Kalbers

Loyola Marymount University

Abstract:

In the past decade, accounting scandals and financial reporting errors have led to heightened awareness of the need for IT controls and legislation of control regimes. In the United States, the Sarbanes–Oxley Act of 2002 (SOX) was one of the early initiatives to legislate internal controls over financial reporting. Many countries and regions have followed with similar legislation. In this tutorial we present an analysis of the prior work on error prevention and detection in spreadsheets as it relates to SOX and IT governance frameworks, more generally. SOX requires publicly traded companies to address the problem of spreadsheet management and to assume some accountability for generating accurate information from spreadsheets for financial reporting. We attempt to reconcile requirements for SOX with IT spreadsheet research. Gaps in design and implementation of spreadsheet controls are identified. From our review of prior work on spreadsheets, we offer a series of options for controlling the spreadsheet development process. Finally, we provide suggestions to help IT practitioners in organizations look beyond SOX regulations at governance of end-user developed content.

Keywords: spreadsheet errors, internal controls, IT governance, regulatory compliance

Volume 27, Article 28, pp. 541-560, October 2010

I. INTRODUCTION

End-users develop applications to support their work or the work of other end-users, with spreadsheets being the most commonly used tool for end-user application developments [Taylor et al., 1998; Eckerson and Sherman, 2008]. Spreadsheets provide a natural interface for model building, are easy to use in terms of inputs, solutions, and report generation, and allow users to perform what-if analysis. The wide range of applications and base of end-users has made spreadsheets a universal modeling platform. By developing an application in the spreadsheet environment, the model can be circulated among a wide range of users without concern about specialized software packages and learning curves. While the different spreadsheet packages and versions are not identical, they are compatible enough that they can support the basic function of each other's models and thereby not impair the widespread use of a developed model. With the arrival of the Internet, web-based spreadsheet packages, such as Google Docs and Spreadsheets, have appeared that allow users to upload, create, and edit spreadsheets online and collaborate with others in real time.

Organizations rely heavily on spreadsheet applications for both information processing and decision making. Spreadsheets within organizations have proliferated in recent years as data warehousing and enterprise resource planning systems have generated spreadmarts, which are defined as "data shadow systems in which individuals collect and massage data on an ongoing basis to support their information requirements or those of their immediate workgroup" [Eckerson and Sherman, 2008]. Spreadmarts are most frequently created in spreadsheets by business analysts and power users who are proficient with Microsoft Excel and, therefore, use this tool quickly to manipulate the data without having to conform to corporate standards for naming conventions and metric calculations. A recent report shows that over 90 percent of organizations have an average of twenty to thirty spreadmarts [Eckerson and Sherman, 2008]. IT professionals worry that spreadsheet proliferation increases an organization's risk of inconsistent data, since undefined and uncoupled data is floating around in various spreadsheets and being used in decision-making. Eighty percent of IT professionals want to eliminate spreadmarts, as an audit trail does not exist with spreadsheets and the time needed to identify and correct potential data discrepancies results in a loss of productivity and higher costs for the organization [Petti and Cannon, 2008]. At the same time, 60 to 80 percent of affected analysts and managers view spreadmarts as a good solution for their business needs. As a result, executive mandates to eliminate spreadmarts or stop IT support for them usually do not successfully stop spreadsheet proliferation within the organization.

The availability and ubiquity of spreadsheets throughout most organizations has also spurred apprehension about the accuracy and integrity of the results produced by a spreadsheet. Research shows that errors are prevalent in spreadsheets [e.g., Panko, 1998, 2006; Panko and Ordway, 2005; Caulkins et al., 2007]. Empirical studies report that 86–100 percent of operational spreadsheets contain errors, often of a costly nature [EuSprRIG]. Lab and field studies suggest that spreadsheet developers create errors accidentally in 2 percent to 5 percent of spreadsheet cells on average, regardless of their experience [Panko and Sprague, 1998]. Large organizations can have thousands of spreadsheets distributed across the enterprise that have been developed by independent end-users in an uncontrolled environment. Due to the nature of end-user computing, spreadsheets, therefore, are also susceptible to fraud. Studies show that it is difficult to detect misstatements once they exist, partly due to the highly polished presentation of the results afforded by the spreadsheet [Galletta et al., 1993, 1996]. Detailed testing can be extremely laborious even with specialized spreadsheet auditing software [Butler 2000a]. Ironically, the ease of use and the widespread availability that makes spreadsheets so popular are the same attributes that also make them susceptible to errors and fraud.

Because spreadsheet programs lack the embedded logic and data controls necessary to prevent errors and misuse, organizations must apply manual or automated control processes to help mitigate spreadsheet risks. As more sophisticated IT tools are created to manage spreadsheets (e.g., add-in auditing tools, Microsoft.Net, business intelligence tools), protocols and processes within an organization need to be implemented to ensure that the tools are used to minimize, detect, and resolve errors in the most effective way possible. The nature and main benefits of end-user development are resistive to attempts to control and restrict the development, sharing, and use of self-generated models, even when organizations communicate the serious problems that can occur with spreadsheets developed through independent, uncoordinated, and undisciplined approaches. In the United States, regulations emerging from the Sarbanes–Oxley Act of 2002 (SOX) require increased attention to IT controls by management. Controls over end-user developed spreadsheet models have come to the forefront because SOX requires publicly traded companies to verify that controls for spreadsheets used in the financial reporting process are in place. In

2004, several surveys reported that 80–95 percent of U.S. firms use spreadsheets for financial reporting [Panko, 2006]. Thus, many publicly traded companies are forced to view end-user developed spreadsheet models that impact financial reporting similar to formal information systems used for financial reporting. Although we focus on the United States and SOX as our reference, IT governance and regulation is relevant globally. Many countries and regions have followed SOX with similar legislation.

In this article, we begin with a discussion of control frameworks, particularly as required by SOX regulations, and present an overview of spreadsheet management in organizations. Next we present the IT literature associated with different spreadsheet controls. In light of the robust control requirements mandated by SOX regulations and analysts' and managers' resistance to adopting a different toolset, we then outline options that companies can consider to manage spreadsheets. Finally we make calls for support of research to help develop some of these options further so that organizations can overcome the problems associated with spreadsheet proliferation and be more motivated to look beyond SOX regulations at their governance of end-user developed content.

II. BACKGROUND

Overview of SOX and IT Governance Frameworks

Adequate controls and appropriate governance mechanisms have long been of interest to organizations, stakeholders, and regulators. Various financial frauds and scandals during the past two decades have led to increased emphasis on governance and controls in organizations. Although frameworks and recommendations have been generated to support voluntary changes in governance and related controls, many new laws and rules have been passed by legislators and regulators. In the U.S., the Sarbanes–Oxley Act of 2002 (SOX) [U.S. Congress, 2002] initiated new policies, procedures, and disclosures for publicly held companies. Other regions and countries implementing new regulations and disclosures include China (C-SOX), the European Union (EuroSox), and Japan (J-SOX). Table 1 presents a summary of significant U.S. and global documents, entities, and legislation that have influenced general and IT governance and controls in organizations. Figure 1 presents a timeline for key events and documents that have impacted IT governance and controls, directly or indirectly, since 1992, with emphasis on the U.S.

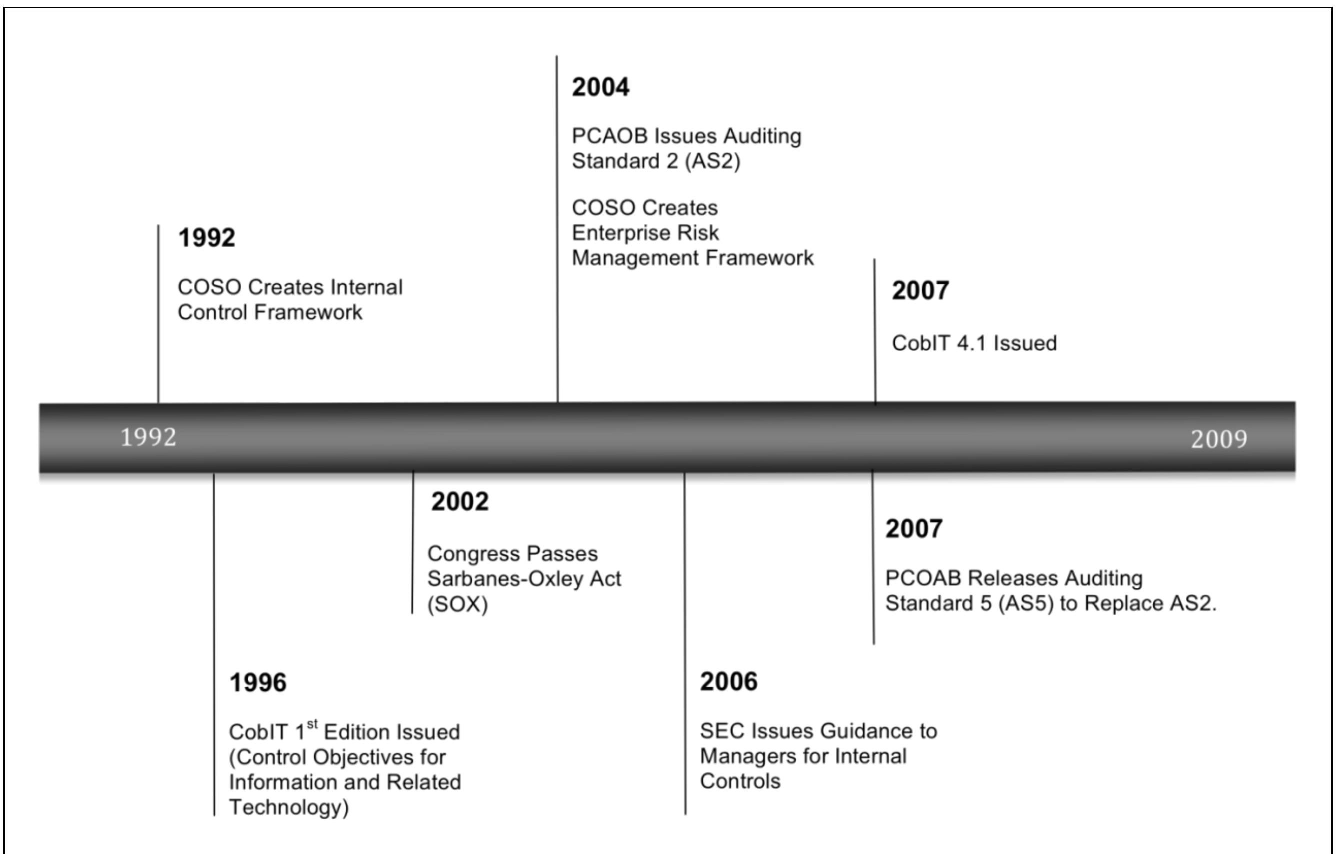

Figure 1. SOX and IT Governance Timeline

Table 1: Self-Regulatory and Regulatory Environment for Governance and Internal Controls—Selected Documents, Entities, and Legislation	
Name	**Description**
China Legislation	Sometimes referred to as "C-SOX," China released *The Basic Standard for Enterprise Internal Control* in May 2008. It became effective in July 2009.
Committee of Sponsoring Organizations of the Treadway Commission (COSO)	COSO is sponsored by the American Accounting Association, American Institute of Certified Public Accountants, Financial Executives Institute, Institute of Management Accountants, and the Institute of Internal Auditors. COSO was formed in 1985. Its initial purpose was to support the work and report of the National Commission on Fraudulent Financial Reporting (Treadway Commission). The Treadway Commission report was issued in 1987. COSO has issued additional reports on fraud and guidance on internal control and enterprise risk management. COSO's internal controls concepts and structure developed in its 1992 *Internal Control—Integrated Framework* has been adopted as the model for auditors in evaluating internal controls in organizations for purposes of reporting on the effectiveness of internal controls required by SOX. It was also used as a foundation for developing legislation in Japan (see "Japan Legislation" below). In 2004, COSO issued more comprehensive guidance in *Enterprise Risk Management—Integrated Framework*. [www.coso.org]
Control Objectives for Information and Related Tech-nology (COBIT)	Globally, COBIT is the most widely accepted internal control framework for IT. The first and second editions were published in the 1990s under the auspices of ISACA. ITGI, which is affiliated with ISACA, is responsible for the third and fourth editions, published in 2000 and 2005. COBIT 4.1 was issued in 2007. [www.itgi.org]
European Union Directives	The European Union's Statutory Audit Directive (2006/43/EC) and Company Reporting Directive (2006/46/EC) are often referred to as *EuroSox.* However, the substance and necessary compliance with these directives have many differences from SOX. Also, the European Union's process for implementing directives is delegated to each member country. These directives were to become effective in 2008, but it is thought that not all countries implemented the directives on a timely basis.
Information Systems Audit and Control Associa-tion (ISACA)	ISACA, formed in 1967, is a global organization for information governance, control, security, and audit professionals. It sponsors several certifications, including Certified Information Systems Auditor (CISA). [www.isaca.org]
IT Governance Institute (ITGI)	ITGI, established in 1998, is a global leader in IT governance and is responsible for publishing COBIT. [www.itgi.org]
Japan Legislation	Sometimes referred to as *J-SOX,* Japan enacted the *Financial Instruments Exchange Law* in June 2006. It became effective for reporting years beginning on or after April 1, 2008.
Public Company Accounting Oversight Board (PCAOB)	The PCAOB is a private-sector, nonprofit corporation, created by the Sarbanes–Oxley Act of 2002. It has authority to oversee auditors of public companies. As part of its activities, it establishes auditing standards for registered public accounting firms. Issued in 2004, Auditing Standard 2 (AS2) was the initial auditing standard issued as guidance to auditors for auditing and reporting on the effectiveness of internal control over financial reporting. Auditing Standard 5 (AS5), issued in 2007, replaced those guidelines. [www.pcaob.org]
Sarbanes–Oxley Act of 2002 (SOX) **Section 302** **Section 404**	The Sarbanes–Oxley Act of 2002 (SOX) is legislation passed in July 2002 by the United States Congress in reaction to major accounting scandals. Two sections of SOX are particularly relevant to this research study. Section 302 requires the principal executive officer(s) and financial officer(s) to take responsibility to maintain and report quarterly on the effectiveness of the company's internal control over financial reporting. Section 404 requires management to assess and report on the effectiveness of the company's internal control as of end of the company's most recent fiscal year, and the company's external auditor to audit and report on the effectiveness of the company's internal control over financial reporting as part of its annual audit report on financial statements. (Also see 10-K and 10-Q below.)
U.S. Securities and Exchange Commission (SEC)	The SEC was created as part of the Securities Exchange Act of 1934. It is responsible for, among other things, regulating stock markets and the reporting of financial information by publicly traded companies in the U.S. [www.sec.gov]
10-K and 10-Q	Most U.S. public companies are required to file certain reports with the SEC on a prescribed basis. These reports include the 10-K and 10-Q. The annual report on Form 10-K provides a comprehensive overview of the company's business and financial condition and includes audited financial statements. Since 2004, independent accountants have also reported on the effectiveness of internal controls as part of the 10-K, as required by Section 404 of SOX. The 10-Q is a public company's unaudited quarterly financial statements for the three quarters prior to its annual filing (10-K). Since 2003, as part of the 10-Q, management is required by Section 302 of SOX to self-report on the effectiveness of internal control. [www.sec.gov]

Section 404 is the most relevant provision in SOX for IT controls. It requires both management and independent accountants to report on effectiveness of internal controls over financial reporting (ICFR).[1] Auditing Standard 2 [Public Company Accounting Oversight Board, 2004] adopted the internal control framework devised by the Committee of Sponsoring Organizations of the Treadway Commission [COSO 1992] as its model for evaluating ICFR. COSO describes internal control in the following way:

> 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 objectives in the following categories:
>
> - Effectiveness and efficiency of operations
> - Reliability of financial reporting
> - Compliance with applicable laws and regulations [COSO, 1992]

COSO's view of internal control goes well beyond a framework for SOX compliance, which is most closely related to the second category, reliability of financial reporting. Although the Public Company Accounting Oversight Board (PCAOB) refers to COSO as a framework for evaluating ICFR, many companies and auditors have adopted Control Objectives for Information and Related Technology (CobiT) [IT Governance Institute, 2007] to address IT compliance for SOX [Blum, 2005]. CobiT was designed for a much broader approach to IT controls than compliance with SOX. The IT Governance Institute (ITGI) views information technology as an integral part of an organization's approach to controlling all three of the COSO categories, and "sustains and extends the organization's strategies and objectives" [IT Governance Institute, 2007, p. 3].

COSO recognized the need for an even more comprehensive assessment of internal controls and risks and issued *Enterprise Risk Management—Integrated Framework*, which broadens the context of internal controls to incorporate risk management throughout the organization [COSO, 2004]. These risk and internal control frameworks may be viewed as complementary and supportive in providing guidance to organizations in meeting their goals, objectives, and responsibilities in very general and specific ways, including compliance with SOX [Damianides, 2005; Panko, 2006; Moeller, 2008]. For example, the CobiT control framework may be adapted to apply specifically to spreadsheets [Butler, 2001]. Spreadsheets may also be integrated into the assessment of internal controls and SOX compliance using the CobiT model [IT Governance Institute, 2006].

In the first two years of implementation, there were many complaints from companies about the significant costs for companies to comply with the detailed testing and documentation required by Section 404 of SOX. The SEC and PCAOB subsequently moved from a "checklist" approach to a "top-down, risk-based approach," including "entity-level controls" for assessing and reporting on internal control over financial reporting for both management and auditors [Securities and Exchange Commission, 2006; PCAOB, 2007]. An audit of internal controls now considers specific financial statement assertions related to specific controls, along with materiality and higher-level controls that may be in place, so that decisions can be made about which controls should be tested for purposes of SOX. This scoping/top-down approach should be used to determine which spreadsheets should be evaluated for purposes of SOX, as not all spreadsheets are of the same importance and risk. "The objective is to identify those spreadsheets that are most significant to the financial reporting process and determine if controls are in place and whether they are tested in a reasonable manner" [IT Governance Institute, 2006, p. 104].

In sum, SOX has been a major impetus for companies to examine controls over spreadsheets, particularly those related to financial reporting. The broader approaches to controls found in the COSO and CobiT frameworks provide a basis to consider policies and procedures for all spreadsheet applications within an organization. In the next section, we more specifically address spreadsheet misstatements and how SOX applies to them.

Overview of Spreadsheet Misstatements and Deficiency Classifications

Misstatements can occur accidentally or intentionally. Most spreadsheet IT research studies document the types and frequencies of accidental errors and attempt to classify the errors based on their attributes into various taxonomies [e.g., Panko and Sprague, 1998; Powell et al., 2008a; Rajalingham et al., 2001]. Spreadsheet errors are often mapped into two general categories of quantitative versus qualitative errors. Quantitative errors are the most commonly documented type in lab and field studies. They result in immediate incorrect numerical bottom-line values

[1] The SEC has delayed requirements of Section 404 for certain small company filers, known as *non-accelerated filers*. Our use of the term *publicly held* in this article will refer to those companies that are subject to all SOX requirements at the time this is written.

and often occur as the result of an omission, a deletion, a formula alteration, erroneous logic, or the duplication of an input assumption. Qualitative errors do not result immediately in incorrect numerical values, but the design flaws of the spreadsheet increase the chance of an eventual quantitative error or misinterpretation during the model's use in its business function. Examples of errors in this category include semantic errors, in which information is unintentionally distorted or ambiguous, making it easy to misinterpret, as well as jamming errors, in which input data is hard-coded into formulas, thereby hiding assumptions and values that may need to be changed by the user. Documenting different types of errors and understanding how they occur can help IT researchers identify effective controls and processes, such as testing protocols and design standards, that will minimize the frequency and impact of errors and maximize the likelihood of their detection.

Fraud, on the other hand, occurs when the misstatement is made with the intent to deceive and create harm. While fraudulent misstatements can be classified in the taxonomies described, the user creating the misstatement will try to minimize the likelihood of detection. Thus, different types of internal controls, such as separation of duties and tighter access controls, are needed to mitigate the potential opportunity for fraudulent misstatements [Mittermeir, et al., 2005].

Measuring (1) the likelihood and (2) the severity of a misstatement in a spreadsheet, whether of an accidental or fraudulent nature, is necessary for an organization to assess the risk of a spreadsheet and to be compliant with accounting standards and regulations. For purposes of financial reporting and SOX compliance, Auditing Standard 5 (AS5) states:

> A **deficiency** in internal control over financial reporting exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent or detect misstatements on a timely basis [PCAOB, 2007, p. 432, paragraph A3].
>
> A **material weakness** is a deficiency, or a combination of deficiencies, in internal control over financial reporting, such that there is a **reasonable possibility** that a material misstatement of the company's annual or interim financial statements will not be prevented or detected on a timely basis [PCAOB, 2007, p. 434, paragraph A7].
>
> A **significant deficiency** is a deficiency, or a combination of deficiencies, in internal control over financial reporting that is less severe than a material weakness, yet important enough to merit attention by those responsible for oversight of the company's financial reporting [PCAOB, 2007, p. 434, paragraph A11].

The Financial Accounting Standards Board (FASB), the body that sets U.S. accounting standards, considers an item material if a financial statement user's decision would be affected by the "magnitude" of the "inclusion or correction of the item" [FASB, 1980, paragraph 132]. Quantitative materiality benchmarks often used in audit practice vary from 2.5 percent to 10 percent of income [Chen et al., 2008]. Materiality has qualitative, as well as quantitative, attributes and must be considered within the context of the particular situation [AICPA, 2006].

Overview of Spreadsheet Control Policies

Misstatements are created at different stages of the spreadsheet life cycle, and the incidence of errors varies by stage. Errors occur during the development and review of the model, throughout the model's use, and as the result of requested modifications or unauthorized alterations to the original model.

Prior to SOX, surveys of MIS executives and spreadsheet developers found that few organizations had formal policies on end-user or spreadsheet development [Panko, 1998]. Companies reported that, while informal guidelines were more common, they still existed in only about half of the organizations. Neither the formal rules nor the informal guidelines were usually implemented and enforced throughout any of the development, testing, auditing, and modification stages of the spreadsheet life cycle, despite all of the literature on the prevalence of spreadsheet errors in organizations. More recent surveys show that most organizations still have no formal policies to ensure spreadsheet quality, reflecting that the organizational attitude toward spreadsheet management has not changed much in general since 1998 [Caulkins et al., 2007; Lawson et al., 2009]. One area in which the corporate culture has changed is financial reporting. Now that SOX regulations hold publicly traded companies accountable for implementing and evaluating their spreadsheet controls for financial reporting, the important question is not whether controls are being implemented, but whether they are being implemented effectively. PCAOB's AS 5 identifies the need for a combination of preventive and detective controls to prevent and detect errors or fraud in financial reporting [PCAOB, 2007].

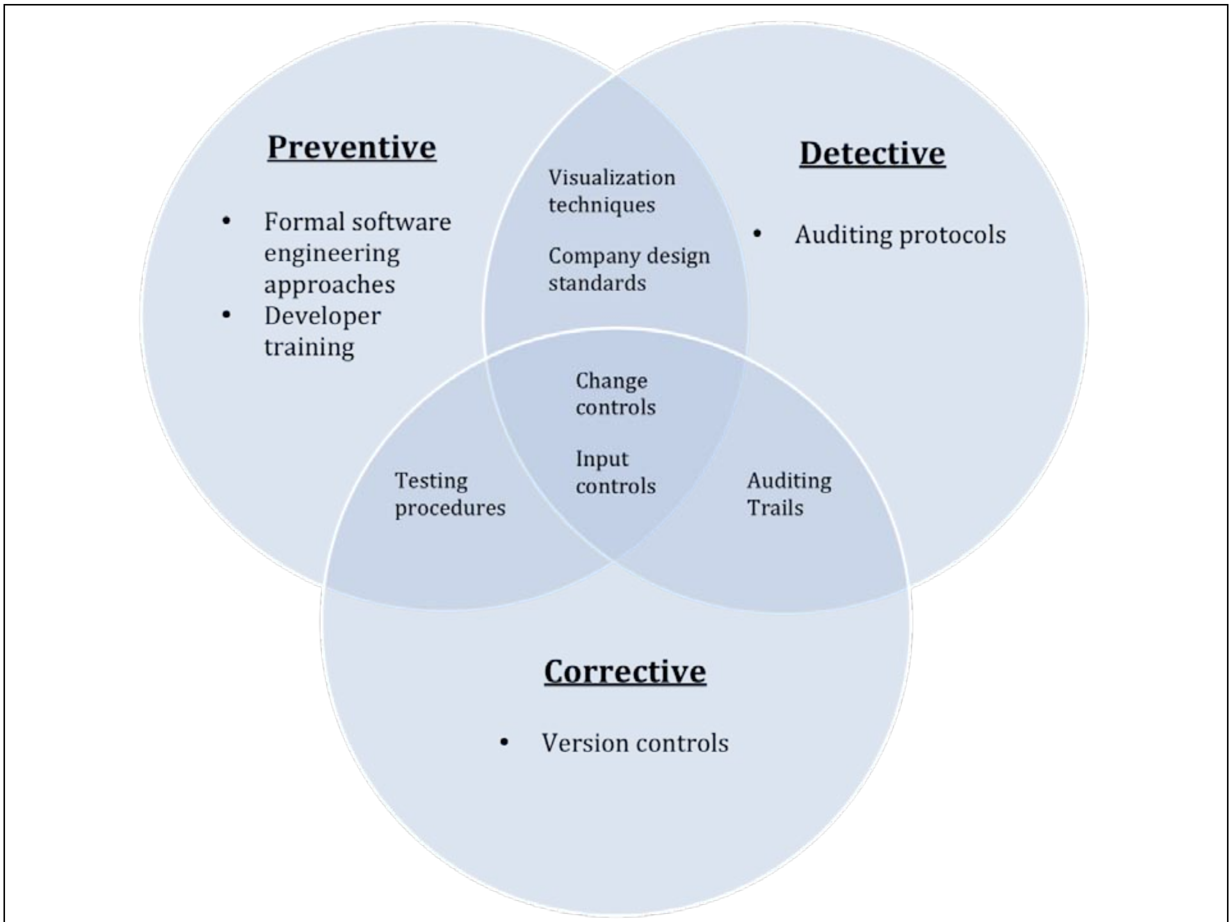

Figure 2. Examples of Controls That Can Be Considered for Different Processes

Panko [2006] proposes to help organizations produce accurate financial reports by minimizing the likelihood of misstatements in a spreadsheet at different stages of development and usage. His approach concentrates on three processes: preventive, detective, and corrective. Figure 2 provides examples of the types of controls that can be considered for implementation in the three processes.

The organization needs to identify and implement effective controls for all three processes to meet their goal of producing financial reporting spreadsheets without any material weaknesses or significant deficiencies. General types of controls that can be considered include change controls, version controls, access controls, input controls, security and integrity of data, documentation, development lifecycle, back-ups, archiving, logic inspection, segregation of duties, and overall analytics [PricewaterhouseCoopers, 2004]. Identifying effective strategies for combining and implementing various controls will mitigate the risks inherent in the spreadsheet environment. The accountability that SOX imposes makes it critical for companies to consider how these different types of controls should be operationally implemented, which includes defining who should be responsible for their implementation and for monitoring their effectiveness.

III. THE IMPACT OF SOX ON SPREADSHEET MANAGEMENT

In order to comply with SOX, companies need to document, evaluate, and test internal controls for spreadsheets that are critical for financial reporting. While many companies that use spreadsheets are not publicly-held and do not fall under the scope of SOX, similar requirements are being imposed by other regulating agencies (e.g., Federal Deposit Insurance Corporation Improvement Act, 1991). When external audit firms identify material weaknesses in a company's financial reporting process a description of the weakness or deficiency is documented in the company's annual 10-K report. Companies reporting material weaknesses in internal control from 2002–2005 "tend to be smaller, younger, financially weaker, more complex, growing rapidly, or undergoing restructuring" [Doyle et al., 2007, p. 193]. Similarly, companies with reported IT deficiencies under Section 404 of SOX are smaller and pay higher audit fees [Grant et al., 2008]. The stock market has been found to react negatively to management disclosure of internal control weaknesses required under Section 302 of SOX [Hammersley et al., 2008]. Companies that report internal control deficiencies have higher cost of equity than those companies that do not [Ashbaugh-Skaife et al., 2009].

Audit Analytics is a public company intelligence service that provides detailed research on over 20,000 public companies. Based on the companies included in their database, there were 113 10-Ks that recorded material weaknesses as the result of inadequate spreadsheet controls for seventy-seven different companies between 2004 and the first half of 2008. For example, in 2006, Design Within Reach was identified as having the following material weakness: "Specifically, controls were not designed and in place throughout the year to ensure that access was restricted to appropriate personnel and that unauthorized modification of the data or formulas within spreadsheets was prevented" [Design Within Reach Inc. 10-K, 2006]. The external audit firms have provided documented guidance that no one in the organization is assuming accountability for spreadsheet risk management [Protiviti Inc., 2008].

Accountability for spreadsheet control deficiencies is important because it is the standard approach to accounting and auditing processes. Ultimately, senior management is the party that will be held accountable for the identified deficiencies. It is critical that the senior executive communicates an end-user computing policy to define the spreadsheet risk management requirements he/she expects from the organization [PricewaterhouseCoopers, 2004]. This policy must define effective processes and enact appropriate monitoring to ensure compliance with these processes. From this policy, an operating model defining accountability, roles and responsibilities, processes, controls, and control standards can be created [O'Beirne, 2005]. The focus then is on documenting the controls, processes and their usage.

PricewaterhouseCoopers and the IT Governance Institute propose that organizations use a high-level five step process to manage spreadsheet risk [PricewaterhouseCoopers 2004]:

1. Create an inventory of spreadsheets that are in the scope of SOX regulations.
2. Perform a risk assessment of financial misstatement (materiality and likelihood) by evaluating the use and complexity of the spreadsheet.
3. Determine the necessary level of controls for "key" spreadsheets.
4. Evaluate existing controls for each spreadsheet.
5. Develop action plans for remediating control deficiencies.

This five-step process is proposed from an auditing perspective, but IT research should provide guidance for the third step. The literature analysis in the next section identifies areas where further research is needed to help practitioners identify more effective controls. In particular, to identify the necessary level of controls and accountability in an operating model, an organization must clearly define the roles and responsibilities of different organizational stakeholders. There are five types of stakeholders associated with spreadsheets in an organization who should be considered in the organization's operating model: the designer, IT, the business user, independent review groups, and internal auditors.

The spreadsheet designers (developers and end-users) develop, implement, update, test, and make spreadsheets operational. Designers should be able to identify and assess the operational risk in their spreadsheets, but they need controls and processes to make sure that the development risks are reasonably mitigated (e.g., formal software development procedures). IT provides infrastructure and software critical to the operation of the spreadsheet. IT needs controls and processes to ensure that sharing, accessing, archiving, backing up, and data are available and safe (e.g., vault server products such as Sharepoint). The business users (e.g., analysts and controllers) use spreadsheet models to generate outputs. They need to review controls to make sure that appropriate financial standards are included in a model, that input and output validity checks are done, and that the appropriate model version is being used. Spreadsheet review groups, as suggested by Miricle Solutions [Miric, 2009], are trained to review and comment on spreadsheets used throughout the organization. They can be responsible for one-time integrity testing of a spreadsheet as well as for setting up and monitoring protocols, processes, and controls for designers and users. Spreadsheet review groups do not always exist within an organization, but, when they do, they are often positioned in internal auditing or IT audit departments. Internal auditors, who provide an independent assessment to senior management of whether or not the spreadsheet risk within the organization is being effectively managed, identify ineffective or missing controls, and perform gap analysis and suggest remediation.

While PricewaterhouseCooper's five-step process was outlined for key spreadsheets associated with financial reporting, research on effective controls and processes is applicable to other key spreadsheets in an organization and, therefore, should be considered in developing best practices for IT governance. As organizations work to comply with SOX regulations, they will identify effective processes, policies, and procedures for spreadsheets associated with financial reporting. The lessons learned will make companies more efficient in general, and this knowledge can be used to improve the general governance structure for end-user computing.

IV. EXISTING IT RESEARCH

PricewaterhouseCoopers and other external auditors, along with IT researchers, have collectively identified a comprehensive list of internal controls that can be considered for spreadsheet risk management [Pricewater-houseCoopers, 2004]. The question is, given the organizational stakeholders involved and the nature of spread-

Table 2: IT Literature Classifications

Controls for Different Stakeholders	Preventive (e.g., SDLC)	Detective (e.g., Auditing)	Corrective (e.g., Change)
Designer End-user (self-designed); Developer (single/multiple)	Anastasakis et al. [2008] Ayalew et al. [2000] Beaman et al. [2005] Bewig [2003] Caulkins et al. [2005] Chadwick et al. [2001] Conway and Ragsdale [1997] Edwards et al. [2000] Hodnigg et at. [2004] Isakowitz et al. [1995] Janvrin and Morrison [2000] Kreie et al. [2000] Kruck [2005] Lawson et al. [2009] McGill and Klobas [2005] Morrison et al. [2003] O'Donnell [2001] Paine [2004] Panko [1998] Panko and Halverson [1997] Panko and Ordway [2005] Pryor [2004] Raffensperger [2003] Rajalingham et al.[2000a, 2000b] Rust et al. [2006] Scheubrein [2003] Vemula et al. [2006]	Clermont [2003] Panko and Sprague [1998] Teo and Tan [1999]	Pryor [2004] Teo and Tan [1999]
User Organization End-user	McGill & Klobas [2005]	Bishop and McDaid [2008] Butler [2000a] Chan et al. [2000] Galletta et al. [1993] Galletta et al. [1997] Grant et al. [2003] Howe and Simkin [2006] Teo and Lee-Partridge [2001]	
IT	Iyer et al [2005] Olzak [2006] Rose [2007] Van Hasselt [2005]	Nash et al [2003] O'Beirne [2008] Panko and Ordway [2005]	Martin [2005] Nash et al. [2003]
Spreadsheet Review Group/Internal Auditor	Bordelon [2006] Martin [2005] Olzak [2006] Panko and Ordway [2005]	Bordelon [2006] Butler [2000b] Chan et al. [2000] Clermont [2002, 2003] Mittermeir et al. [2005] Nash et al. [2003] O'Beirne [2008] Panko and Ordway [2005] Powell et al. [2008b]	Martin [2005] Murphy [2006] Nash et al.[2003]

sheets, how can this research on internal controls be organized into a coherent framework that will further develop effective implementation of the controls? We propose that Panko's three identified processes be used in conjunction with the organizational stakeholders to create a framework for classifying IT research. We reviewed recent existing literature on managing spreadsheets, focusing on research done since SOX and covering the key areas pertaining to the three processes identified by Panko. The articles reviewed were placed into one or more cells in the framework based on whether the elements of control pertaining to that cell were discussed in the paper or not. The framework and the papers that fall into each cell are shown in Table 2.

In Table 2, each column represents a process and each row represents an organizational stakeholder. As spreadsheet review groups do not always exist in an organization or are embedded inside internal auditing departments, it is difficult to clearly delineate these two roles and so the two stakeholders have been merged into the last row grouping. IT research is classified inside this framework table based on the process the spreadsheet control supports and the stakeholder who could be held responsible for that particular process. For example, assigning multiple developers to work separately on the same spreadsheet task and then cross-checking their results with each other increases the accuracy of the final model [Vemula et al., 2006]. Vemula's paper suggests a control procedure for spreadsheet developers that will reduce development errors, and, therefore, the paper is categorized in the Preventive Control/Designer portion of Table 2.

It is apparent from Table 2 that IT research is heavily focused on developing some intuitive matches, such as preventive controls for spreadsheet designers and detective controls for spreadsheet review groups. This table also shows that there are some areas where minimal IT research has been done, such as for the general category of corrective controls, as well as for preventive user controls. One explanation for these gaps is that the category application can be partly covered by research efforts done in another category. For example, testing techniques, such as unit testing and system review, were proposed for preventing development errors made by designers [Pryor, 2004]. These testing procedures may also be applied when models are modified after release.

Table 3: Controls Identified for the Designer Throughout Different Lifecycle Processes

Controls for Different Stakeholders	Preventive(e.g., SDLC)	Detective (e.g., Auditing)	Corrective (e.g., Change)
Designer End-user (self-designed); Developer (single/ multiple)	• Best design practices • Expert-novice differences • Surveys of spreadsheet practices and corporate policies • Effect of teaching design principles and system development methods • Impact of designer's spreadsheet knowledge on the successful use of a spreadsheet application • Graphical approaches such as data flow diagrams and influence diagrams • Visualization techniques • Design strategies to improve usability • Tips for using Excel built-in controls • Organizational quality control procedures • Axioms for improving spreadsheet accuracy • Algorithm to capture logic • Applying formal software engineering development procedures such as SDLC • Validation methodologies and efforts • Testing vs. code review • Test driven development • Discovering spreadsheet structure • Spreadsheet engineering processes	• Heuristics for visually identifying irregularities • Framework of error risks	• Testing vs. code review • Framework of error risks

The classifications in Table 2 are also based on the organizational stakeholder formally identified in the paper. It cannot be assumed that these stakeholders will remain the same throughout the three proposed lifecycle processes. In order to minimize the chances of misstatements (both intentional and accidental) at the corrective stage, the testing procedures should be part of a change control that includes specification for separation of duties between the spreadsheet designer, the user and an independent party, such as the spreadsheet review group [Read and Batson, 1999; Pricewaterhouse Coopers, 2004]. Thus, controls and procedures can be applied to multiple processes (see Figure 2) with different organizational stakeholders assuming responsibility for implementation. There can be a potentially negative impact on the effectiveness of the control or procedure if an organization does not consider carefully which stakeholder should be responsible for implementing the control. For example, the ability to detect errors is dependent on the reviewer's prior incremental practice with spreadsheet error detection [Teo and Lee-Partridge, 2001], and, therefore, different testing procedures would be necessary for a spreadsheet developer, user, and an independent review group.

Tables 3 and 4 list examples of general controls that have been proposed for different stakeholders, providing more illustrations of overlap and gaps in the research. Table 3 highlights research that measures whether experience, training, and testing in general decrease spreadsheet designers' errors.

Table 4: Controls Identified for Stakeholders Other Than Designers

Controls for Different Stakeholders	Preventive(e.g., SDLC)	Detective(e.g., Auditing)	Corrective (e.g., Change)
User Organization End-User	• Impact of spreadsheet knowledge on the successful use of a spreadsheet application	• Proposed visualization and auditing tools • Methods to ensure data integrity for microarray data management • Expert-novice differences • Impact of prominence of errors and electronic environment • Quantifying risk • Understanding end-user behavior in debugging	
IT	• Error prevention techniques • Spreadsheet development life cycle • Review of commercial spreadsheet products • Business intelligence tools to share spreadsheets and centralize data • Web service to manage models • Survey of spreadsheet issues and corporate policies	• Keeping track of changes in a spreadsheet • Computer aided audit tools and techniques	• Keeping track of changes Detailed controls
Spreadsheet Review Group/ Internal Auditor	• Error prevention techniques • Spreadsheet development life cycle • Specific tips for Internal Auditors on using Excel controls • Detailed examples of controls and procedures • Broad recommendations for procedures and controls • Spreadsheet testing and fraud prevention	• Controls for fraud • Auditing protocol; • Specific tips on using Excel built-in controls • Criteria for classifying a spreadsheet's risk • Broad recommendations for procedures and controls; keeping track of changes • Visualization techniques for non-modular designs and data mining • Data quality control techniques	• Keeping track of changes • Detailed controls • A review process that assesses whether changes can be made while maintaining model integrity

While preventive controls investigating these tools are categorized as applicable for the spreadsheet designer in Tables 2 and 3, the resulting model quality should also have an indirect preventive impact on the user which is currently not reflected in Tables 2 and 4. Similarly, Table 4 lists research suggesting that internal auditors should recommend design standards and protocols for the organization; the research speculates that if standards are established and followed, development errors would decrease with standardized training, remaining errors would be easier to detect by independent review groups, and users would experience a lower cognitive load as all models would be written with the same design standards [Martin, 2005]. Again, potential indirect impacts of the primary control are not captured in Tables 2 through 4.

There are some important gaps in Tables 2 through 4 that also need to be addressed in future IT research. Effectively managing corrections is critical for SOX compliance as well as for general best practice for IT governance. Effective input controls for users are also important so as to ensure that valid data inputs are utilized and the integrity of the model outputs is maintained. Comparatively little research exists that investigates the effectiveness of information and data quality controls for spreadsheet users, in either the preventive or detective process. This is particularly critical for organizations concerned with minimizing the risk of fraud in their financial and operational spreadsheets as well as the risk of the decoupled data associated with spreadmarts. The gaps identified in Tables 2 through 4 are mirrored in actual organizational implementations of spreadsheet controls. A survey of various quality control methods at forty-five businesses showed that most organizations were not implementing techniques (e.g., input controls, auditing tools, tracking changes, cell protection) to manage spreadsheets once the models were operational or to support detective and corrective functions [Caulkins et al., 2007].

Similarly, of the 113 10-Ks reporting SOX material weaknesses for inadequate internal control of spreadsheets between 2004 and mid-2008, forty-two weaknesses were associated with inadequate review processes (detective processes), forty-one weaknesses with inadequate access controls, twenty-seven weaknesses with inadequate change management controls, and twenty-two weaknesses with lack of data integrity controls. Only nine material weaknesses were associated with inadequate spreadsheet testing, and none of the weaknesses specifically targeted preventing misstatements in the design process, though this area is where the most IT research is being done. Fifty of the 113 10-Ks reporting SOX material weaknesses did not identify specific control issues but stated in general terms that the company did not maintain effective controls over their spreadsheets. (Note: some 10-K reports were identified with more than one internal control weakness, so the total weaknesses reported exceed 113.)

These deficiency statistics reflect the areas of emphasis that external auditors place on key spreadsheets associated with financial reporting for SOX compliance and may not be representative of broader shortcomings for general spreadsheet management. For example, spreadsheets developed to support strategic and operational decision-making often require more focus on design controls due to the complexity of the model's logic and the what-if analysis that will be performed by users. Tables 2 through 4 show that IT research is addressing issues such as design controls that are important for spreadsheets, but it is also missing some critical processes for spreadsheets, especially in financial reporting, and this lack of knowledge contributes to the ineffective implementation of controls being documented in practice.

V. SPREADSHEET CONTROL OPTIONS FOR ORGANIZATIONS TO CONSIDER

The rest of this article outlines control options that practitioners should consider throughout the spreadsheet lifecycle and identifies critical areas where further research is needed to support the bridge between accounting regulation and a broader implementation of spreadsheet controls. For example, while it is clear from the literature review and the 10-K reports that IT research is needed to help identify effective processes for managing spreadsheets after they have been developed, frustrations on the part of IT professionals with spreadsheet proliferation and low organizational productivity suggest that the development process is not being well managed either. The options outlined in this section provide general guidelines for evaluating the effectiveness of the controls currently implemented in an organization along with other controls companies should consider for eventual implementation. These suggestions are not meant to be an exhaustive list of controls that should be considered, but rather serve as a starting point for managing spreadsheets in an organization.

In applying the high-level five-step process to manage spreadsheet risk [PricewaterhouseCoopers, 2004], not all spreadsheets need to be controlled identically. While SOX requires companies to identify and control spreadsheets that have a reasonable chance of resulting in a material misstatement associated with financial reporting, organizations often have other mission-critical spreadsheets that need similar levels of established controls, given the importance, extended use, complexity, and number of users of the spreadsheet. While IT research is being done to design taxonomies of spreadsheets for organizations so that they can identify spreadsheets that need greater or lesser degrees of control [Madahar et al., 2007], the options proposed in this section are framed generally to address how different levels of controls could be applicable to spreadsheets in various types of classifications.

Options for Controlling the Spreadsheet Development Process

First, it is important for a company to evaluate the type and amount of spreadsheet training that has been invested in the end-users developing the spreadsheet models. Empirical lab studies show that training spreadsheet users on basic spreadsheet design principles significantly reduce qualitative design errors, though not quantitative errors [Beaman et al., 2005; Kreie et al., 2000]. Reducing qualitative errors, however, makes a model more usable throughout the spreadsheet's lifecycle, as well as easier to audit, especially if later data discrepancies or quantitative errors are identified. Developing a well-designed spreadsheet model reduces the risk that a user will misinterpret the results of the spreadsheet or generate a quantitative error while using the model. For spreadsheets that are meant to be reused or shared with others, these design aspects become a critical control for preventing errors on the parts of the users, as well as improving the eventual productivity of the party responsible for auditing or changing the model. However, a developer survey shows that very little training is provided by organizations for spreadsheet development [Lawson et al., 2009].

Training for end-users is a very effective strategy. A one-day seminar on basic design principles, such as effective layout strategies, cell documentation, cross-footing techniques, and not embedding numbers in formulas, would result in noticeable long-run productivity gains for an organization, because it is easy to incorporate these concepts into future models once the end-user understands the principles. For end-users who are generating mission-critical spreadsheets that will be repeatedly used and shared with others, additional training on more advanced design features, such as conditional formatting, data validation, and form controls, is also highly recommended. Also, for the end-users who are creating spreadsheet-based spreadmarts to perform more advanced analysis and business intelligence, training on advanced modeling tools such as Excel's built-in auditing feature, pivot tables, data tables, and database functions would be beneficial. While these types of advanced tools require more development time and a higher learning curve, training end-users on the best way to implement these techniques will help organizations ensure that the analysis is being done as productively and robustly as possible in the spreadsheet environment.

Second, companies need to create design standards and/or guidelines for the spreadsheet models that will be shared or from which reports will be generated. Standardizing design features such as layout approaches, color and formatting styles, documentation, and cell naming conventions will reduce the cognitive load of the eventual users and auditors. This will make the logic of the model and its assumptions and outputs easier to follow and comprehend. IT professionals or internal auditors need to define a spreadsheet style policy that is explicit about methods, functions, and formats, similar to the example provided in O'Beirne [2005]. Providing end-users with training and incentives to abide by the spreadsheet development policy will create a consistent style throughout the organization, thereby increasing organizational productivity as the spreadsheet is put into operational use.

Finally, organizations should consider various preventive procedures to ensure that the logic, formulas, and calculations programmed by the developer are accurate. Formal approaches decrease errors in structured programming for general IT development projects. While IT research argues that errors in spreadsheets should decrease with the implementation of formal software engineering approaches, empirical evidence has not been produced to broadly support this claim. In one empirical lab study, participants were trained on a specific design approach for a specific error type (using Data Flow Diagrams for linked errors), which resulted in lower error rates for that error type [Janvrin and Morrison, 2000]. Another study showed that the group creating influence diagrams had fewer omission errors than the control group [O'Donnell, 2001]. However, in addition to requiring advanced training, these formal specification and development techniques may impose such a high cognitive load on the end-user, who is not used to developing models in a structured manner, that gains in the error reduction typically associated with the approach are offset by new errors created by cognitive processing difficulties. Cognitive load has been a problem for other software development and usage and is potentially a problem for spreadsheets as well [Bible et al., 2005; Turetkin and Schuff, 2006].

However, IT research does clearly show that testing is a necessary formal development approach for reducing the risk of quantitative spreadsheet errors [Panko and Ordway, 2005]. For mission-critical spreadsheets, a detailed test plan should be institutionalized that defines "who applies what test cases to the spreadsheet, when, and how" [O'Beirne, 2005]. While there are no specific methods that have been clearly identified as being the most effective (e.g., test cases versus code inspection), IT research concludes that the testing should be done by someone other than the developer to maximize chances of error detection [Caulkins et al., 2005; Panko and Halverson, 1997]. This means that organizations need to be willing to commit to budget time and personnel resources to perform these formal review procedures before a mission-critical spreadsheet is put into operational use.

Further IT research is needed to help practitioners understand how to control the spreadsheet development process so that the resulting spreadsheet can be productively integrated into operational use. A call for research is needed in three general areas. First, extended research must be done on classification of qualitative errors and their impacts on various parties throughout the spreadsheet lifecycle so that practitioners can prioritize their use of resources and training as effectively as possible. Second, while design principles for readability, module layout, jamming, and data management exist [Caulkins et al., 2005; Conway and Ragsdale, 1997; Edwards et al., 2000, Panko, 1988], readability requires further exploration since conflicts between criteria for user and developer readability have been noted. For example, user readability improves when input assumptions are displayed close to the outputs they affect, but developer readability is easier when a distinct module section is created for data management purposes, often requiring a separation of the assumptions from the resulting outputs [Raffensperger, 2003]. Similarly, conflicting views on the usefulness of range names exist: range names provide the user with improved readability of the spreadsheet's logic [Bewig, 2003] but simultaneously increase the risk of quantitative design errors, as the range names can be linked to incorrectly defined cell ranges and these errors are extremely hard to detect [Panko and Ordway, 2005]. These and other design controversies need to be examined from the perspective of the developer's and user's cognitive loads, so that again the most effective overall design standards and training can be provided. Finally, IT research should attempt to measure how the cognitive load of the end-user who applies formal development approaches impacts spreadsheet error reduction in order to determine whether a significant error reduction can be realized that would make it worthwhile for organizations to consider institutionalizing these types of approaches.

Options for Controlling the Spreadsheet in Its Operational Use

The 10-K deficiencies summarized in the previous section show that companies need to focus more on ensuring the integrity of key spreadsheets after they are developed by establishing processes to detect user-generated misstatements, prevent risk of misuse and fraud, and manage changes better. In interviews with forty-five senior managers from various industry sectors, five of the seven most commonly mentioned types of spreadsheet errors reported can be generated by users after the model has been successfully developed, including inaccurate data (76 percent), reuse of spreadsheets (49 percent), misinterpretation of outputs or reports (27 percent), broken links (22 percent), and copy/paste errors (22 percent) [Caulkins et al., 2007]. These spreadsheet errors can occur as the result of insufficient input data controls, poor spreadsheet design, corrupted formulas and even fraudulent activities.

First, a company needs to consider which operational spreadsheets should be audited and how this auditing will be done. This requires specifying a procedure for how often a spreadsheet must be reviewed, as well as the organizational party that will be responsible for reviewing the spreadsheet, keeping in mind that separation of duties is an important organizational control for maximizing the chances of detecting accidental misstatements and fraudulent activities. In organizations without independent spreadsheet review groups, independent users may act as the auditing agency. In such cases, training users on detection techniques should be considered because research shows experience with detection increases the number of errors caught [Teo and Lee-Partridge, 2001]. An organization should also consider specifying an auditing protocol for the reviewer to follow to maximize the error detection rate, similar to the steps proposed in Powell et al. [2008b], as well as using third-party auditing tools, such as Spreadsheet Professional. As auditing is expensive and time-consuming, organizations need to develop a process to classify the risk of a spreadsheet created by an external party or end-user, as was done in Butler [2000b], so that only high risk spreadsheets are targeted for review.

IT research shows that, even with the most detailed audits, rarely will all spreadsheet errors be detected [Galletta et al., 1993, 1996; Panko, 1998; Teo and Lee-Partridge, 2001]. The likelihood of detection in the case of fraud is even lower because the originator is intentionally trying to hide the misstatement [Mittermeir et al., 2005]. So while auditing of mission-critical spreadsheets should be seriously considered, establishing resources that prevent user-generated misstatements may be a more effective approach for maintaining spreadsheet integrity. The investment in training and design guidelines that was previously described should improve spreadsheet development, which is one way to prevent user misstatements.

Other options that an organization can consider include the implementation of various IT tools. Aggressive controls, such as separating data from the program, will ensure data integrity and consistency throughout the organization. Centralizing data in a common database where it can be maintained by IT professionals in a consistent XML format for data feeds to Excel applications will let business users maintain the benefits of quick, flexible analysis and presentation generation [Marinos, 2005]. Similarly, as more functionality and flexibility is designed into the spreadsheet components of .NET systems, organizations may have an easier time convincing analysts and users to use these systems more, which will bind spreadsheets to enterprise databases and other .NET data sources. An organization can also consider placing mission-critical spreadsheets in a vault server, where they will be protected by security access controls and strong auditing tools [Nash et al., 2003; Panko, 2006].

Finally, procedural options can be implemented to try to deter fraud and set an appropriate level of security for a spreadsheet. Some suggestions include an operational policy that defines separation of duties, testing procedures and access policies, technology controls to limit access and changes, and data control procedures [Panko and Ordway, 2005]. Such a policy would need to describe procedures for ensuring that the correct version is successfully distributed for use throughout the organization so that all users are not using a spreadsheet with errors or outdated standards. One auditor proposed that more traditional archiving/filename/sharing convention strategies would get spreadsheets reasonably under control, along with procedures for specifying access levels for approved users, reviewers, and developers [Martin, 2005]. There are also procedures for validating data input and controlling data integrity that can be implemented by end-users to overcome some data problems [Grant et al., 2003; Rose, 2007; O'Beirne, 2008].

The possible controls that have been proposed in IT literature for managing the risks of a developed spreadsheet provide a wide range of possible solutions for organizations to consider. However, surveys and recorded SOX deficiencies show that most organizations do not understand how to effectively implement these controls into their operations. This suggests a general call for IT research to document the effectiveness of different proposed tools with respect to their ability to prevent misuse and to provide reasonable accessibility, flexibility, and cost.

VI. CONCLUDING COMMENTS

Spreadsheets are the most commonly used tool for end-user application developments in business. The value of spreadsheet software comes from its ease of use and how it enables most employees to develop and use models of varying degrees of sophistication with limited training. As past studies point out, this exposes organizations to the errors and fraudulent activity that can make its way into the numerous spreadsheets in use at a typical organization. Surveys show that, despite the documented presence of errors in spreadsheets, most organizations still have not established formal guidelines or policies for managing their spreadsheets. SOX and similar legislations in other countries bring the issue of controls on end-user developed spreadsheet models to the forefront as they make publicly traded companies accountable for verifying that effective controls for spreadsheets used in the financial reporting process are in place.

In the literature analysis presented in this article, we show that there is a need to better understand controls for users, such as input and data controls, as well as general detection and change management techniques. Understanding the relationship between an organization's design standards and the impact it will have on designers, users, and reviewers, and the spreadsheet's resulting accuracy, are factors that managers need to consider. This will help organizations structure the training that must be provided to end-users who design, develop, and use spreadsheets in their daily work. Most importantly, there is a need to develop governance methods that allow for better controls without hampering end-user development and usage of spreadsheet models and without imposing prohibitive expenses and time commitments on the organization. As organizations work to comply with financial reporting regulations, like SOX, they are identifying effective processes, policies, and procedures for spreadsheets associated with financial reporting. The lessons learned from this experience can be used to make employees more productive as they use spreadsheets while also improving the general governance structure for end-user computing. Due to the proliferation of spreadsheets and the new technology developments in computing that are occurring, such as cloud computing, these control issues will become even more important in the near future.

Planning and implementing adequate controls for spreadsheets in organizations should go beyond regulatory compliance. Organizations need to understand the effect of standards and policies on the end-users, as well as on those who are responsible for controlling the use of information and systems in the organization. Controls on spreadsheets are likely to lead to conflicts between the end-users and IT professionals who are typically responsible for controlling the systems. The problems associated with controlling spreadsheets discussed in this article go beyond financial reporting and address controls needed for all types of spreadsheets used in an organization. Both end-users as well as IT professionals need to identify and apply effective controls to ensure that spreadsheets remain a practical and useful tool while limiting the risk that organizations face from errors in end-user developed spreadsheet models.

REFERENCES

Editor's Note: The following reference list contains hyperlinks to World Wide Web pages. Readers who have the ability to access the Web directly from their word processor or are reading the article on the Web, can gain direct access to these linked references. Readers are warned, however, that:

1. These links existed as of the date of publication but are not guaranteed to be working thereafter.
2. The contents of Web pages may change over time. Where version information is provided in the References, different versions may not contain the information or the conclusions referenced.
3. The author(s) of the Web pages, not AIS, is (are) responsible for the accuracy of their content.
4. The author(s) of this article, not AIS, is (are) responsible for the accuracy of the URL and version information.

American Institute of Certified Public Accountants (AICPA) (2006) *Audit Risk and Materiality in Conducting and Audit*, *Statement on Auditing Standards,* No. 107, New York, NY: American Institute of Certified Public Accountants.

Anastasakis, L., C.W. Olphert, J.M. Wilson (2008) "Experiences in Using a Contingency Factor-Based Validation Methodology for Spreadsheet DSS", *Journal of the Operational Research Society,* (59)6, pp. 756–761.

Ashbaugh-Skaife, H. et al. (2009) "The Effect of SOX Internal Control Deficiencies on Firm Risk and Cost of Equity", *Journal of Accounting Research* (47)1, pp. 1–43.

Ayalew, Y., M. Clermont, R. Mittermeir (2000) "Detecting Errors in Spreadsheets", *Spreadsheet Risks, Audit and Development Methods* (1), pp. 51–62.

Beaman, I., E. Waldmann, P. Krueger (2005) "The Impact of Training in Financial Modelling Principles on the Incidence of Spreadsheet Errors", *Accounting Education: An International Journal* (14)2, pp. 199–212.

Bewig, P. (2003) "In Excel, Cell Names Spell Speed, Safety", *Journal of Accountancy* (196)3, pp. 68–71.

Bible, L., L. Graham, A. Rosman (2005) "The Effect of Electronic Audit and Environments on Performance", *Journal of Accounting, Auditing and Finance* (20)1, pp. 27–42.

Bishop, B. and K. McDaid (2008) "Spreadsheet Debugging Behavior of Expert and Novice End-Users", *Proceedings of the 4th International Workshop on End-User Software Engineering*, Leipzig, Germany, pp. 56–60.

Blum, D. (2005) "Sarbanes-Oxley: Act Promotes Survival of the Fittest", *Network World*, http://www.networkworld.com/columnists/2005/020705blum.html (current April 11, 2009).

Bordelon, P. (2006) "Safeguarding Spreadsheets", *The Internal Auditor* (63)3, pp. 29–32.

Butler, R. (2000a) "Is This Spreadsheet a Tax Evader? How H.M. Customs & Excise Tax Test Spreadsheet Applications", *Proceedings of the 33rd Hawaii International Conference on System Sciences*, Maui, Hawaii, January 4–7, 2000.

Butler, R. (2000b) "Risk Assessment for Spreadsheet Developments: Choosing Which Models to Audit", *Customs and Excise,* pp. 1–11.

Butler, R. (2001) "Applying the CobiT® Control Framework to Spreadsheet Developments", European Spreadsheet Risks Interest Group, http://arxiv.org/ftp/arxiv/papers/0801/0801.0609.pdf (current April 13, 2009).

Caulkins, J.P., E. Morrison, T. Wiedemann (2005) "Spreadsheet Errors: Are They Undermining Decision Making in Your Organization?" *Public Manager* (34)1, pp. 22–27.

Caulkins, J.P., E.L. Morrison, T. Wiedemann (2007) "Spreadsheet Errors and Decision-Making: Evidence from Field Interviews", *Journal of Organizational and End User Computing* (19)3, pp. 1–23.

Chadwick, D., B. Knight, K. Rajalingham (2001) "Quality Control in Spreadsheets: A Visual Approach Using Color Codings to Reduce Errors in Formulae", *Software Quality Journal* (9), pp. 133–143.

Chan, H.C., C. Ying, C.B. Peh (2000) "Strategies and Visualization Tools for Enhancing User Auditing of Spreadsheet Models", *Information and Software Technology* (42), pp. 1037–1043.

Chen, C., K. Pany, J. Zhang. (2008) "An Analysis of the Relationship Between Accounting Restatements and Quantitative Benchmarks of Audit Planning Materiality", *Review of Accounting and Finance* (7)3, pp. 236–251.

Clermont, M. (2003) "Analyzing Large Spreadsheet Programs", *Proceedings of the 10th Working Conference on Reverse Engineering,* pp. 306–315.

Clermont, M., C. Hanin, R. Mittermeir (2002) "A Spreadsheet Auditing Tool Evaluated in an Industrial Context", *Spreadsheet Risks, Audit and Development Methods* (3), pp. 35–46.

Committee of Sponsoring Organizations of the Treadway Commission (COSO) (1992) *Internal Control–Integrated Framework*, New York, NY: The Committee of Sponsoring Organizations of the Treadway Commission.

Committee of Sponsoring Organizations of the Treadway Commission (COSO) (2004) *Enterprise Risk Management–Integrated Framework: Executive Summary*, New York, NY: The Committee of Sponsoring Organizations of the Treadway Commission.

Conway, D.G. and C.T. Ragsdale (1997) "Modeling Optimization Problems in the Unstructured World of Spreadsheets", *Omega* (25)3, pp. 313–322.

Damianides, M. (2005) "Sarbanes-Oxley and IT Governance: New Guidance on IT Control and Compliance", *Information Systems Management* (22)1, pp. 77–87.

Design Within Reach Inc., Form 10-K (2006) http://www.sec.gov/Archives/edgar/data/1116755/000119312507106080/d10k.htm (current September 8, 2009).

Doyle, J., W. Ge, S. McVay (2007) "Determinants of Weaknesses in Internal Control over Financial Reporting", *Journal of Accounting and Economics* (44), pp. 193–223.

Eckerson, W.W. and R.P. Sherman (2008) "Strategies for Managing Spreadmarts", *Business Intelligence Journal* (13)1, pp. 23–24.

Edwards, J.S., P.N. Finlay, J.M. Wilson (2000) "The Role of OR Specialists in 'Do It Yourself' Spreadsheet Development", *European Journal of Operational Research* (127)1, pp. 14–27.

The European Spreadsheet Risks Interest Group (EuSprRIG) (2009) "Spreadsheet Mistakes—News Stories", http://www.eusprig.org/stories.htm (current September 8, 2009).

Federal Deposit Insurance Corporation Improvement Act of 1991, OMB Circular No. A-123.

Financial Accounting Standards Board (FASB) (1980) *Statement of Financial Accounting Concepts, No. 2,* Stamford, CT: Financial Accounting Standards Board.

Galletta D.F. et al. (1993) "An Empirical Study of Spreadsheet Error-Finding Performance", *Accounting, Management and Information Technologies* (3)2, pp. 79–95.

Galletta, D.F. et al. (1996/1997) "Spreadsheet Presentation and Error Detection: An Experimental Study", *Journal of Management Information Systems* (13)3, pp. 45–63.

Grant, G.R. et al. (2003) "Maintaining Data Integrity in Microarray Data Management", *Biotechnology and Bioengineering* (84)7, pp. 795–800.

Grant, G.H, K.C. Miller, F. Alali (2008) "The Effect of IT Controls on Financial Reporting", *Managerial Auditing Journal* (23)8, pp. 803–823.

Hammersley, J.S., L.A. Myers, C. Shakespeare (2008) "Market Reactions to the Disclosure of Internal Control Weaknesses and to the Characteristics of Those Weaknesses under Section 302 of the Sarbanes Oxley Act of 2002", *Review of Accounting Studies* (47)1, pp. 1–43.

Hodnigg, K., M. Clermont, R.T. Mittermeir (2004) "Computational Models of Spreadsheet Development: Basis for Educational Approaches", *Institut für Informatik-System, Universität Klagenfurt, Austria,* working paper.

Howe, H. and M.G. Simkin (2006) "Factors Affecting the Ability to Detect Spreadsheet Errors", *Decision Sciences Journal of Innovative Education* (4)1, pp. 101–122.

Isakowitz, T., S. Schocken, H.C. Lucas, Jr. (1995) "Toward a Logical/Physical Theory of Spreadsheet Modeling", *ACM Transactions on Information Systems* (13)1, pp. 1–37.

Iyer, B., G. Shankaranarayanan, M.L. Lenard (2005) "Model Management Decision Environment: A Web Service Prototype for Spreadsheet Models", *Decision Support Systems* (40)2, pp. 283–304.

IT Governance Institute (2006) *IT Control Objectives for Sarbanes-Oxley, 2nd edition,* Rolling Meadows, IL: IT Governance Institute.

IT Governance Institute (2007) *CobitT 4.1,* Rolling Meadows, IL: IT Governance Institute.

Janvrin, D. and J. Morrison (2000) "Using a Structured Design Approach to Reduce Risks in End User Spreadsheet Development", *Information & Management* (37)1, pp. 1–12.

Kreie, J. et al. (2000) "Applications Development by End-Users: Can Quality Be Improved?" *Decision Support Systems* (29), pp. 143–152.

Kruck, S.E. (2005) "Testing Spreadsheet Accuracy Theory", *Information and Software Technology* (48), pp. 204–213.

Lawson, B., Baker, K.R., Powell, S.G. Foster-Johnson, L. (2009) "A Comparison of Spreadsheet Users with Different Levels of Experience", *Omega*, (37)3, June 2009 pp. 579-590.

Madahar, M., P. Cleary, D. Ball (2007) "Categorization of Spreadsheet Use Within Organizations, Incorporating Risk: A Progress Report", *Proceedings of the EuSpRIG 2007 Conference*, University of Greenwich, London, England, pp. 37–45.

Marinos, G. (2005) "How the Information Supply Chain Supports Corporate Reporting in the Financial Services Industry", *DM Review* (15)4, p. 22.

Martin, A.G. (2005) "Get Spreadsheets Under Control", *The Internal Auditor* (62)6, pp. 31–35.

McGill, T.J. and J.E. Kobas (2005) "The Role of Spreadsheet Knowledge in User-Developed Application Success", *Decision Support Systems* (39)3, pp. 355–369.

Miric, Adrian, "Part 3: Review Groups Are the Foundation for Dealing with Spreadsheet Risks", http://www.auditexcel.co.za/sox3.html (current September 8, 2009).

Mittermeir, R., M. Clermont, K. Hodnigg (2005) "Protecting Spreadsheets Against Fraud", *Proceedings of the EuSpRIG 2005 Conference*, Greenwich, UK, pp. 69–80.

Moeller, R.R. (2008). *Sarbanes-Oxley Internal Controls: Effective Auditing with AS5, CobiT, and ITIL*, Hoboken, NJ: John Wiley & Sons, Inc.

Morrison, C. et al. (2003) "A Graphical Approach for Reducing Spreadsheet Linking Errors", *Advanced Topic in End User Computing*, Hershey, PA: IGI Publishing, pp. 173–189.

Murphy, S. (2006) "EuSpRIG 2006 Commercial Spreadsheet Review", *Proceedings of the EuSpRIG 2006 Conference*, http://www.eusprig.org/2006/commercial-spreadsheet-review.pdf (current September 6, 2009).

Nash, J.C., N. Smith, A. Adler (2003) "Audit and Change Analysis of Spreadsheets" in Chadwick, D. and D. Ward (eds.) *Proceedings of the 2003 Conference of the European Spreadsheet Risks Interest Group*, Dublin, London: EuSpRIG, pp. 81–90.

O'Beirne, P. (2005) *Spreadsheet Check and Control*, Wexford, Ireland: Systems Publishing.

O'Beirne, P. (2008) "Information and Data Quality in Spreadsheets", *Proceedings of the EuSpRIG 2008 Conference*, pp. 171–185.

O'Donnell, P.A. (2001) "The Use of Influence Diagrams in the Design of Spreadsheet Models: An Experimental Study", *Australian Journal of Information Systems* (9)1, pp. 79–91.

Olzak, T. (2006) "Spreadsheet Assurance", http://www.windowsecurity.com/whitepapers/Spreadsheet-Assurance.html (current September 6, 2009).

Paine, J. (2004) "Spreadsheet Structure Discovery with Logic Programming", *Proceedings of EuSpRIG 2004*, http://www.j-paine.org/spreadsheet_structure_discovery.html (current September 6, 2009).

Panko, R.R. (1988) *End User Computing: Management, Applications, and Technology,* New York, NY: Wiley.

Panko, R.R. (1998) "What We Know About Spreadsheet Errors", *Journal of End User Computing, Special Issue on Scaling Up End User Development* (10)2, Spring 1998, pp. 15–21. Revised May 2008, http://panko.shidler.hawaii.edu/ssr/Mypapers/whatknow.htm (current September 15, 2010).

Panko, R.R. (2006) "Spreadsheets and Sarbanes-Oxley: Regulations, Risks, and Control Frameworks", *Communications of the Association for Information Systems* (17), Article 29.

Panko, R.R. and R.P. Halverson, Jr. (1997) "Are Two Heads Better Than One (At Reducing Errors in Spreadsheet Modeling?)", *Office Systems Research Journal* (15)1, pp. 21–32.

Panko, R.R. and N. Ordway (2005) "Sarbanes–Oxley: What About All the Spreadsheets? Controlling for Errors and Fraud in Financial Reporting", *Proceedings of the EuSpRIG 2005 Conference*, Greenwich, UK, July 7–8, 2005, pp. 15–60.

Panko, R.R. and R.H. Sprague (1998) "Hitting the Wall: Errors in Developing and Debugging a 'Simple' Spreadsheet Model", *Decision Support System* (22), pp. 337–353.

Petti, R.J. and H.I. Cannon (2008) "An Innovative Spreadsheet Authoring Environment", *Journal of Internet Banking and Commerce* (13)2, pp. 1–11.

Powell, S.G., K.R. Baker, B. Lawson (2008a) "A Critical Review of the Literature on Spreadsheet Errors", *Decision Support Systems* (46), pp. 128–138.

Powell, S.G., K.R. Baker, B. Lawson (2008b) "Developing an Auditing Protocol for Spreadsheet Models", *Information Management* (45)5, pp. 312–320.

PricewaterhouseCoopers (2004) "The Use of Spreadsheets: Considerations for Section 404 of the Sarbanes-Oxley."

Protiviti Inc. (2008) *Spreadsheet Risk Management: Frequently Asked Questions Guide,* http://now.eloqua.com/e/f2.aspx?elqFormName=hidden&elqSiteID=361&id=us-rsg1&doc=http://www.protiviti.com/en-US/Insights/Resource-Guides/Documents/SpreadsheetRiskMgmtFAQ09.pdf (current September 6, 2009).

Pryor, L. (2004) "When, Why and How to Test Spreadsheets*", Proceedings of the EnSpRIG 2004*, pp. 145–152.

Public Company Accounting Oversight Board (2004) *Auditing Standard No. 2—An Audit of Internal Control over Financial Reporting Performed in Conjunction with an Audit of Financial Statements* (as of October 1, 2008), http://www.pcaobus.org/Rules/Rules_of_the_Board/Auditing_Standard_2.pdf (current April 11, 2009).

Public Company Accounting Oversight Board (2007) *Auditing Standard No. 5—An Audit of Internal Control over Financial Reporting That Is Integrated with an Audit of Financial Statements* (as of October 1, 2008), http://www.pcaobus.org/Rules/Rules_of_the_Board/Auditing_Standard_5.pdf (current April 11, 2009).

Raffensperger, J.F. (2003) “New Guidelines for Spreadsheets”, *International Journal of Business and Economics* (2)2, pp. 141–154.

Rajalingham, K. et al. (2000a) “Efficient Methods for Checking Integrity: An Integrated Spreadsheet Engineering Methodology (ISEM)”, *Integrity and Internal Control in Information Systems: An Integrated Spreadsheet Engineering Methodology,* pp. 41–58.

Rajalingham, K. et al. (2000b) “Quality Control in Spreadsheets: A Software Engineering-Based Approach to Spreadsheet Development”, *Proceedings of the 33rd Annual Hawaii International Conference on Systems Sciences* (HICSS-33), pp. 1–9.

Rajalingham, K, D. Chadwick, B. Knight (2001) “Classification of Spreadsheet Errors”, *Symposium of the European Spreadsheet Risks Interest Group EuSpRIG 2001: Virginia Conference*, pp. 1–12.

Read, N. and J. Batson (1999) “Spreadsheet Modelling Best Practice”, *Institute of Chartered Accountants in England and Wales* (ICAEW).

Rose, J. (2007) “Taking Human Error out of Financial Spreadsheets”, *Strategic Finance* (88)9, pp. 52–55.

Rust, A., B. Biship, K. McDaid (2006) “Investigating the Potential of Test-Driven Development for Spreadsheet Engineering”, *Proceedings of the EuSpRIG 2006 Conference*, pp. 95–105.

Scheubrein, R. (2003) “Elements of End-User Software Engineering”, *INFORMS Transactions on Education* (4)1, pp. 1–23, http://ite.pubs.informs.org/Vol4No1/Scheubrein/ (current September 6, 2009).

Securities and Exchange Commission (SEC) (2006) “Management’s Report on Internal Control over Financial Reporting”, http://www.sec.gov/rules/proposed/2006/33-8762.pdf (current April 11, 2009).

Taylor, M.J., E.P Moynihan, A.T. Wood-Harper (1998) “End-User Computing and Information Systems Methodologies”, *Information Systems Journal* (8), pp. 85–96.

Teo, T.S.H. and J.E. Lee-Partridge (2001) “Effects of Error Factors and Prior Incremental Practice on Spreadsheet Error Detection: An Experimental Study”, *Omega* (29), pp. 445–456.

Teo, T.S.H. and M. Tan (1999) “Spreadsheet Development and ‘What-if’ Analysis: Quantitative versus Qualitative Errors”, *Accounting, Management and Information Technology* (9), pp.141–160.

Turetken, O. and D. Schuff (2006) “The Impact of Context-Aware Fisheye Models on Understanding Business Processes: An Empirical Study of Data Flow Diagrams”, *Information and Management* (44), pp. 40–52.

U.S. Congress (2002) “Sarbanes-Oxley Act of 2002”, http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_bills&docid=f:h3763enr.tst.pdf (current on April 11, 2009).

Van Hasselt, C. (2005) “Solutions That Make Excel Behave”, *Treasury and Risk Management* (15)2, p. 15.

Vemula, V.R., D. Ball, S. Thorne (2006) “Towards a Spreadsheet Engineering”, *Proceedings of the EuSpRIG 2006 Conference*, pp. 53–64.

ABOUT THE AUTHORS

Linda A. Leon is an Associate Professor of Applied Information Management Systems in the College of Business Administration at Loyola Marymount University, Los Angeles, CA. She received her business economics degree and her Ph.D. in management science from the University of California, Los Angeles. Her current research interests include managerial decision support using spreadsheets, controlling spreadsheet errors, evaluating technology for improving teaching, and supply chain management. She has published in journals such as *Interfaces*, *OR Insight*, *Decision Sciences Journal of Innovative Education* and *INFORMS Transactions on Education*.

Dolphy M. Abraham is a Professor of Systems and Operations Management at Alliance Business School (ABS), Bangalore, India. He was the Dean of Academics at St. Joseph's College of Business Administration, Bangalore, India, and a Professor of Computer Information Systems in the College of Business Administration at Loyola Marymount University, Los Angeles, USA, prior to joining ABS. He received his Ph.D. in Business from the Joseph M. Katz Graduate School of Business, University of Pittsburgh. His current research interests are in the areas of knowledge management, controlling spreadsheet errors, social network analysis, and quality of end-user developed content.

Lawrence Kalbers is the R. Chad Dreier Chair in Accounting Ethics and the Director of the Center for Accounting Ethics, Governance, and the Public Interest in the College of Business Administration at Loyola Marymount University. His research interests include corporate governance, ethics, professionalism, auditor burnout, auditor organizational commitment, accounting education, and accounting history. His research has been published in *Accounting and Business Research*, *Accounting Education: An International Journal, Accounting Educators' Journal, Accounting Today*, *Advances in Accounting Behavioral Research, Auditing: A Journal of Practice and Theory*, *Critical Perspectives on Accounting*, *Internal Auditor*, *Journal of Accountancy, Journal of Accounting Education*, *Journal of Managerial Issues, Management Accounting*, *Managerial Auditing Journal*, *Mid-American Journal of Business*, *The Ohio CPA Journal*, and *Review of Accounting and Finance*.

Communications of the Association for Information Systems

ISSN: 1529-3181