Decision Support Systems 54 (2012) 452–460

Contents lists available at SciVerse ScienceDirect

Decision Support Systems

journal homepage: www.elsevier.com/locate/dss

A spreadsheet life cycle analysis and the impact of Sarbanes–Oxley

Linda Leon [a,*], Lawrence Kalbers [a], Nancy Coster [a], Dolphy Abraham [b]

[a] Loyola Marymount University, 1 LMU Drive, College of Business Administration, Los Angeles, California 90045-2659, USA
[b] Alliance University, School of Business, Chikkahegde Cross, Chandpura-Anekal Main Road, Anekal, Bangalore 562 106, India

ARTICLE INFO

Article history:
Received 1 March 2012
Received in revised form 22 May 2012
Accepted 19 June 2012
Available online 27 June 2012

Keywords:
Spreadsheet
Spreadsheet life cycle
Controls
Sarbanes–Oxley
IT governance

ABSTRACT

Past studies show that only a small percent of organizations implement and enforce formal rules or informal guidelines for the planning, design and development, usage, modification, and disposition stages of spreadsheet models. Due to the lack of such policies, there has been little research on how companies can effectively govern spreadsheets throughout their life cycle. This paper describes a survey involving 43 participants from the United States, representing companies that were working on compliance with the Sarbanes–Oxley Act of 2002 (SOX) as it relates to spreadsheets for financial reporting. The findings of this survey describe specific controls that organizations have implemented to manage spreadsheets for financial reporting throughout a spreadsheet's life cycle. Our findings indicate that there are problems in all stages of a spreadsheet's life cycle and we suggest several important areas for practice and future research.

1. Introduction

It is broadly accepted that errors are prevalent in spreadsheets [13,17]. Spreadsheet risk can be defined as the likelihood of adverse operational or financial consequences resulting from the use of a spreadsheet. To date, most spreadsheet research has focused primarily on understanding and mitigating spreadsheet risks associated with quantitative errors that occur during system development, an early stage of the system's life cycle. This line of research investigates and often suggests implementation of more formal software engineering techniques during the creation of a spreadsheet [4,9,13]. While there are definite risks of developing an erroneous spreadsheet, there are additional and equally as serious risks associated with the maintenance and operational use of the spreadsheet throughout the later parts of its life cycle. We use a broad life cycle framework for our study, which includes planning, design and development, usage, modification, and disposition of a spreadsheet, in order to provide a lens for developing our survey and evaluating the results.

We surveyed 43 companies working on compliance with the Sarbanes–Oxley Act of 2002 (SOX) as it relates to spreadsheets associated with financial reporting. We chose to sample such companies because of the regulatory, financial, and reputational importance of spreadsheets used for financial reporting under SOX. That is, for these spreadsheets that are associated with government regulation and are monitored by external auditors, we expect best organizational practices. We collected information about the controls and processes they have implemented in their organizations as well as the difficulties and challenges they have encountered. This paper presents the findings of this survey. While these findings describe spreadsheets associated with financial reporting, the identification of effective controls and processes are applicable to other key spreadsheets in an organization and therefore should be considered in developing best practices for IT governance. Similarly, there are areas where organizations fail to reasonably control the spreadsheets used in financial reporting, despite their efforts. We expect that all organizations will encounter the same challenges and difficulties that these organizations are facing, but many non-regulated companies will avoid addressing risk until there is an easy and effective way of dealing with the problem.

The remainder of the paper is divided into five parts. The next section provides an overview of the spreadsheet life cycle, controls, and the accountability SOX introduces that motivates organizations to implement controls and processes for spreadsheet development and use. A life cycle framework is proposed from which controls can be considered. The survey methodology is then discussed and the results of the survey are described and analyzed. Finally, conclusions and suggestions for practice and future research are made as we identify the areas where companies are struggling to effectively control spreadsheets.

2. Overview of the spreadsheet life cycle, controls, and SOX accountability

2.1. General background

Panko and Halverson [15] outlined a taxonomy of spreadsheet research issues as a three dimensional cube, in which one important

* Corresponding author. Tel.: +1 310 338 7634; fax: +1 310 338 3000.
E-mail addresses: Linda.Leon@lmu.edu (L. Leon), Lawrence.Kalbers@lmu.edu (L. Kalbers), Nancy.Coster@lmu.edu (N. Coster), dolphy.abraham@alliance.edu.in (D. Abraham).

0167-9236/$ – see front matter © 2012 Elsevier B.V. All rights reserved.
doi:10.1016/j.dss.2012.06.006

dimension was the system life cycle stage. They defined this life cycle as consisting of four stages: cell entry, draft of model, debugging, and operational. The first three stages detailed their interpretation of the system development life cycle. Their review of previous research studies documented observations associated with auditing/monitoring, user controls, modifications, and different party responsibilities in the operational stage. As a first step in the outlined research plan presented in their paper, they created a separate taxonomy of development and testing error types for the system development life cycle stages [16]. Panko and Aurigemma [14] later revised this taxonomy, but noted the shortcoming that the *system life cycle* dimension was not addressed in either version; their studies did not examine a spreadsheet's ongoing use after development. In the taxonomy proposed by Rajalingham, Chadwick & Knight [20], errors that end-users can make, such as data entry errors or interpretation errors, as well as the user's intention to create fraud, were considered. This taxonomy represented a first attempt to define and classify spreadsheet risks during operational use. Since then, the increased emphasis on IT governance has led to the identification of issues that contribute to the risk of a spreadsheet after its development, such as maintenance, documentation, version control, privacy issues, and reasonable separation of duties.

Basic spreadsheet programs lack the embedded logic and data controls necessary to prevent errors and misuse during operational use. Therefore, organizations need to apply manual or automated control processes to help mitigate spreadsheet risks by ensuring that appropriate tools are used to minimize, detect, and resolve errors throughout the entire life cycle. In general, end-users are resistive to attempts to control and restrict the development, sharing, and use of self-generated models. The challenge is to identify effective controls that can help an organization improve the integrity of its spreadsheets without the controls being prohibitively time-consuming or expensive to implement and without interfering with the benefits of the spreadsheet medium.

Surveys show that most organizations have no formal policies to ensure the integrity of their operational spreadsheets [2,7,12,17]. Companies reported that while informal guidelines were common, formal guidelines existed in only about half of the organizations. Neither the formal rules nor the informal guidelines were usually implemented and enforced throughout the planning, development, usage, modification, and disposition stages of the spreadsheet life cycle, despite all of the literature on the prevalence of spreadsheet errors in organizations. One area where the corporate culture has changed is in financial reporting [22]. Sarbanes–Oxley regulations hold publicly traded companies in the U.S. accountable for implementing and evaluating their spreadsheet controls for financial reporting. The Public Company Accounting Oversight Board's (PCAOB) Auditing Standard 5 identifies the need for a combination of preventive and detective controls to prevent and detect errors or fraud in financial reporting [19]. In 2004, several surveys reported that 80–95% of U.S. firms use spreadsheets for financial reporting [13]. Thus, Sarbanes–Oxley regulations force many publicly traded companies to view end-user developed spreadsheet models that impact financial reporting similar to formal information systems used for financial reporting.

2.2. Background of SOX and controls

In the U.S., as a result of various financial frauds and scandals over the past two decades, the Sarbanes–Oxley Act of 2002 (SOX) [23] initiated new policies, procedures, and disclosures in financial reporting for publicly held companies. For years ending on or after November 15, 2004, 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. 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 77 different companies between 2004 and the first half of 2008 [9]. For example, in 2006, Design Within Reach Inc. 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" [3].

With SOX, organizations are being held accountable for the first time to provide documentation about the effectiveness of their spreadsheet risk management practices for the entire spreadsheet life cycle. In particular, the external audit firms focus on existing spreadsheets and identify control deficiencies primarily for the stages after the spreadsheet is developed. Senior executives should communicate an end-user computing policy to define the spreadsheet risk management requirements expected from the organization [18]. This policy must define effective processes and enact appropriate monitoring to ensure compliance with these processes. Most importantly, these processes need to encompass all stages of the system life cycle. From this policy, an operating model defining accountability, roles and responsibilities, processes, controls, and control standards can be created [11]. Finally, the company should document implementation of the controls and processes outlined in the operating model. In order to do this, it is necessary to elaborate on what Panko and other spreadsheet researchers previously defined simply as the "operational" stage.

3. Developing the spreadsheet life cycle framework

It is advisable for companies to adopt a framework as a foundation for developing policies and procedures for spreadsheet controls. Many companies and auditors have adopted Control Objectives for Information and Related Technology (CobiT) [6] to address IT compliance for SOX [1]. Other useful guidance for the development and assessment of spreadsheets also exists. The Institute of Internal Auditors recently issued a practice guide for user-developed applications (UDAs), which includes guidelines for controlling and auditing UDAs using a risk-based assessment of financial, operational, and compliance materiality [5]. To manage spreadsheet risk, PricewaterhouseCoopers [18] proposes that organizations create an inventory of spreadsheets that are in the scope of SOX regulations, evaluate the use and complexity of each spreadsheet to assess the risk of financial misstatement, determine the necessary level of controls for "key" spreadsheets, evaluate existing controls for these spreadsheets, and develop action plans to remediate control deficiencies.

General types of controls that can be considered for implementation include change controls, version controls, access controls, input controls, security and integrity of data, documentation, development life cycle, back-ups, archiving, logic inspection, segregation of duties, and overall analytics [18]. These control activities can be embedded within and across different life cycle stages of the spreadsheets. Panko [13] suggests a framework where control activities are classified into three broad categories: preventive, detective, and corrective controls. Applying this framework assumes that the individuals associated with a spreadsheet throughout its life cycle can identify appropriate control activities from these three sets, and properly segregate responsibilities, to mitigate the risk of an error at each stage.

The accountability that SOX imposes makes it critical for companies to consider how these different types of controls should be implemented in their operations, and includes defining who should be responsible for their implementation and for monitoring their effectiveness. An organization should clearly define the roles and responsibilities of different organizational stakeholders. This includes developers, business users, business owners (who are defined as the people responsible for having the spreadsheet developed), IT and IS security officers, independent review groups, the accounting department, and internal auditors. It is often the case, however, that one person performs several roles, such as