JOURNAL OF INFORMATION SYSTEMS
Vol. 26, No. 2
Fall 2012
pp. 189–213

American Accounting Association
DOI: 10.2308/isys-50255

The Updated COSO Internal Control—Integrated Framework: Recommendations and Opportunities for Future Research

Diane J. Janvrin
Iowa State University

Elizabeth A. Payne
University of Louisville

Paul Byrnes
Rutgers, The State University of New Jersey

Gary P. Schneider
Quinnipiac University

Mary B. Curtis
University of North Texas

ABSTRACT: To address the changing business environment and increased shareholder interest, the Committee of Sponsoring Organizations of the Treadway Commission (COSO) recently issued an exposure draft updating its 1992 *Internal Control—Integrated Framework*. We review the updated *Framework* and discuss the comments we (as the Environmental Scanning Committee of the American Accounting Association's Information Systems Section) offered COSO regarding how to improve the *Framework*. In addition, we identify research opportunities for accounting information system scholars related to the new *Framework*.

Keywords: Internal Control Framework; COSO Framework; IT controls; outsourcing.

I. INTRODUCTION

In response to changes in business and operating environments, advances in technology, increased market globalization, and increased shareholder interest, the Committee of Sponsoring Organizations of the Treadway Commission (COSO) recently issued an exposure draft updating the internal control framework it developed in 1992. Incorporating insights from professionals in industry, academia, government agencies, and non-profit organizations, the

We thank Kevin Kobelsky and Vernon Richardson for their input on this project.

Editor's note: Accepted by J. Donald Warren.

Published Online: July 2012

updated *Framework* is intended to help organizations develop and maintain systems of internal control that are adaptable to changes in the business and operating environments (COSO 2011). The new *Framework* retains the original's core definition of internal control, its five components of internal control (control environment, risk assessment, control activities, information and communication, and monitoring), and its three objectives of internal control (operations, reporting, and compliance). In contrast to the original framework, the new *Framework* codifies internal control components into explicitly stated principles and attributes.

This paper has three objectives. First, we discuss the similarities and differences between the original and the updated *Framework*. Second, we discuss the comments we (as the Environmental Scanning Committee of the American Accounting Association's Information Systems Section) offered COSO regarding how to improve the *Framework*.[1] Third, we identify research opportunities for accounting information systems scholars related to the new *Framework*.

Our paper provides several contributions to the accounting information systems literature. First, although widely accepted by organizations and auditors (COSO 2011), the original 1992 framework did not consider explicitly internal control concepts related to information technology. Given the rapid growth in technology and the need for businesses to adapt to new technologies, examining how the new *Framework* integrates information technology into internal control concepts should be of interest to the accounting information systems community. Further, academic input into the *Framework* development process is important. The *Framework* raises a number of issues that could benefit from future research. We identify a number of issues and specific research questions that arise from them. Finally, the *Framework* provides a new perspective for discussing internal control concepts in accounting information systems courses.

We proceed as follows. First, we present background information and describe how the revised *Framework* differs from the original 1992 framework. Next, we evaluate the proposed *Framework* and offer suggestions for future research. Finally, we conclude by discussing implications and identifying research limitations.

II. BACKGROUND

In reaction to the noteworthy frauds uncovered early in the 21st century (e.g., Enron and WorldCom), the U.S. Congress passed the Sarbanes-Oxley Act of 2002 (SOX, U.S. House of Representatives 2002). This law mandated an attestation of internal control effectiveness by corporate executives (§404(a)) and an external audit of internal control in conjunction with the audit of financial statements (§404(b)). Additionally, SOX created the Public Company Accounting Oversight Board (PCAOB) to regulate the previously self-regulated public accounting profession (§101). The PCAOB established specific requirements for internal control attestation including the audit of internal control over financial reporting by external auditors (PCAOB 2007a), and the evaluation and classification of internal control errors (deficiencies, significant deficiencies, and material weaknesses).

Although audit standards for non-public companies (established by the Auditing Standards Board [ASB] of the American Institute of Certified Public Accountants [AICPA]) do not require management or the external auditor to attest to the operating effectiveness of internal control over financial reporting as is required by the PCAOB, they do require auditors to gain an understanding of the entity's system of internal control (AICPA 2006). Further, although neither PCAOB nor AICPA standards require management or the auditor to use a specific

[1] Our complete comments can be found at: http://www.ic.coso.org/Lists/UploadedFiles/Attachments/102/32429804-b142-4676-94f5-052d8b01b57c_Information%20Systems%20Section%20-%20American%20Accounting%20Association%20-%20%20Responses%20for%20COSO.pdf

internal control framework in carrying out their responsibilities, both organizations do require the use of an internal control framework and reference the (original) COSO framework as a suitable framework to be used (AICPA 2006; PCAOB 2007a). Thus, organizations predominantly use the COSO framework, although this was not its intended purpose. Therefore, to make the framework more applicable to its new role and to address changes in business and operating environments, COSO issued a draft of a revised *Framework* in December 2011.

The *Framework*'s objective is to "enable organizations to effectively and efficiently develop and maintain systems of internal control that can enhance the likelihood of achieving the entity's objectives and adapt to changes in the business and operating environments" (COSO 2011, i). These changes in business and operating environments include "expectations for governance oversight; globalization of markets and operations; changes in business models; demands and complexities in laws, rules, regulations, and standards; expectations for competencies and accountabilities; use of, and reliance on, evolving technologies; and expectations relating to preventing and detecting corruption" (COSO 2011, i).

III. SIMILARITIES TO AND DIFFERENCES FROM ORIGINAL 1992 *FRAMEWORK*

The *Framework* retains its original definition of internal control, the five components of internal control (control environment, control activities, risk assessment, information and communication, and monitoring), as well as the three categories of internal control objectives (operations, reporting, and compliance). *Operation objectives* pertain to the effectiveness and efficiency of the organization's operations including operations and financial performance goals and safeguarding assets against loss (COSO 2011, 3). *Reporting objectives* refer to producing reliable reports and include internal, external, financial, and nonfinancial reporting, while *compliance objectives* pertain to adherence to laws and regulations the organization is subject to (COSO 2011, 3). The *Framework* expands the original "financial reporting objective" since it now recognizes all types of reporting (internal, external, financial, and nonfinancial).

The most notable change to the *Framework* is its codification of the internal control components into 17 principles (and their related attributes) as shown in Exhibit 1.

IV. EVALUATING THE PROPOSED *FRAMEWORK* AND SUGGESTIONS FOR FUTURE RESEARCH

In our comment letter to COSO, we offered recommendations designed to improve the *Framework*. In the process of reviewing and commenting on the *Framework*, we also recognized many opportunities for future research that we summarize in Exhibit 2. In this section we discuss the recommendations made and the resulting research opportunities. Our discussion is organized into four categories: one for the Overall *Framework* and one each for three of the internal control components, specifically Control Environment, Risk Assessment, and Monitoring Activities.

Overall *Framework*

Several suggestions to COSO and research opportunities fall under the Overall *Framework* category. Specifically, we are concerned about the lack of technology integration, the question of whether control frameworks are effective and efficient, lack of recognition of the relationship between supply chain partners and internal control, and the use of a principles- versus rules-based approach.

EXHIBIT 1

Principles in the Updated COSO *Framework* and Related Attributes[a]

Panel A: Control Environment

1. The organization demonstrates a commitment to integrity and ethical values.
   Attributes:
   - set tone at the top
   - establish standards of conduct
   - evaluate adherence to standards of conduct
   - address deviations in a timely manner
2. The board of directors demonstrates independence of management and exercises oversight for the development and performance of internal control.
   Attributes:
   - establish board of directors oversight responsibilities
   - retain or delegate oversight responsibilities as appropriate
   - apply relevant expertise
   - board of directors operate independently of the organization
   - provide oversight during the development and performance of the system of internal control
3. Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.
   Attributes:
   - consider all structures of the organization (including outsourced service providers)
   - establish reporting lines
   - define, assign, and limit authorities and responsibilities
4. The organization demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.
   Attributes:
   - establish policies and procedures
   - attract, develop, and retain individual
   - evaluate competence and address shortcomings
   - plan and prepare for succession
5. The organization holds individuals accountable for their internal control responsibilities in the pursuit of objectives.
   Attributes:
   - enforce accountability through structures, authorities, and responsibilities
   - establish performance measures, incentives, and rewards
   - evaluate performance measures, incentives, and rewards for ongoing relevance
   - consider excessive pressures
   - evaluate performance and rewards or discipline individuals

[a] Source: COSO 2011

(continued on next page)

Overall Framework *Issue 1: Improve Integration of Technology Issues*

Although one motivation for revising the 1992 framework was to address the use of, and reliance on, evolving technologies, the proposed *Framework* explicitly considers technology issues in only one Control Activity principle. We recommended that COSO more fully integrate technology into the entire *Framework* and provided two examples of technology

EXHIBIT 1 (continued)

Panel B: Risk Assessment

6. The organization specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.
   Attributes:
   - consider toleration for risk and required level of precision/materiality
   - comply with externally established standards and frameworks and laws and regulations
   - reflect management's choices
   - reflect entity activities
   - include operations and financial performance goals
   - form basis for committing of resources
7. The organization identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risk should be managed.
   Attributes:
   - involve appropriate levels of management
   - include entity, subsidiary, division, operating unit, and functional levels
   - analyze internal and external factors
   - estimate significance of risks identified
   - determine how to respond to risks
8. The organization considers the potential for fraud in assessing risks to the achievement of objectives.
   Attributes:
   - consider various ways that fraud can occur
   - consider risk factors
   - assess incentive and pressures
   - assess opportunities
   - assess attitudes and rationalizations
9. The organization identifies and assesses changes that could significantly impact the system of internal control.
   Attributes:
   - assess changes in the external environment
   - assess changes in the business model
   - assess changes in leadership

Panel C: Control Activities

10. The organization selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.
    Attributes:
    - integrate with risk assessment
    - determine relevant business processes
    - consider entity-specific factors
    - evaluate a mix of control activity types
    - consider at what level activities are applied
    - address segregation of duties

(continued on next page)

EXHIBIT 1 (continued)

11. The organization selects and develops general control activities over technology to support the achievement of objectives.
   Attributes:
   - determine dependency between the use of technology in business processes and technology general controls
   - establish relevant technology infrastructure control activities
   - establish relevant security management process control activities
   - establish relevant technology acquisition, development, and maintenance process control activities
12. The organization deploys control activities as manifested in policies that establish what is expected and in relevant procedures to effect the policies.
   Attributes:
   - establish policies and procedures to support deployment of management's directives
   - establish responsibility and accountability for executing policies and procedures
   - perform using competent personnel
   - perform in a timely manner
   - take corrective action
   - reassess policies and procedures

Panel D: Information and Communication

13. The organization obtains or generates and uses relevant, quality information to support the functioning of other components of internal control.
   Attributes:
   - identify information requirements
   - capture internal and external courses of data
   - process relevant data into information
   - maintain quality throughout processing
   - consider costs and benefits
14. The organization internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of other components of internal control.
   Attributes:
   - communicate internal control information with personnel
   - communicate with the board of directors
   - provide separate communication lines
   - select relevant method of communication
15. The organization communicates with external parties regarding matters affecting the functioning of other components of internal control.
   Attributes:
   - communicate to external parties
   - enable inbound communications
   - provide separate communication lines
   - communicate with the board of directors
   - select relevant method of communication

(continued on next page)

issues that have major internal control implications—cloud computing[2] and enterprise resource planning (ERP) systems.

The character of cloud computing itself alters security expectations at every level when compared to previous technologies (Ren et al. 2012). Fundamentally different tools and

[2] Cloud computing is also known as software-as-a-service (SaaS) or platform-as-a-service (PaaS).

EXHIBIT 1 (continued)

Panel E: Monitoring Activities

16. The organization selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.
    Attributes:
    - consider a mix of ongoing and separate evaluations
    - establish baseline understanding
    - consider rate of change
    - use knowledgeable personnel
    - integrate with business processes
    - evaluate objectively
    - adjust scope and frequency
17. The organization evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.
    Attributes:
    - assess results
    - communicate deficiencies to management
    - report deficiencies to senior management and the board of directors
    - monitor corrective actions

---

strategies are required to attain an acceptable level of risk for transaction control in cloud environments (DeFelice 2010; Ren et al. 2012). Further, ERP systems, used by many large organizations and an increasing number of small organizations, require built-in controls uniquely characteristic of these systems (Grabski and Leech 2007; Morris 2011). Organizational dependence on ERP systems requires specific controls that must be "embedded within or linked to ERP systems" (Grabski et al. 2011, 40) to achieve the organization's planning and management control objectives. Again, the issues are fundamentally different from those faced in environments where the computing infrastructure is under the immediate control of the organization.

A significant body of research demonstrates investment in technology matters to investors (Dehning and Richardson 2002; Dehning et al. 2003, 2004, 2005; Kobelsky et al. 2008a; Kobelsky et al. 2008b; Oh et al. 2006), and is important for strategic achievement (Henderson et al. 2010; Nicolaou et al. 2011; Piccoli and Ives 2005; Premkumar et al. 2004) and operational effectiveness (Dehning et al. 2007; Hunton 2002; Hunton et al. 2008). However, technology must be controlled, and these controls become more complex as the technology advances in complexity. Thus, we encouraged COSO to improve integration of technology issues in the *Framework*.

Research opportunities related to integration of technology concerns. Although we noted previously that technology investments are important to investors and assist organizations in strategic achievement and operational effectiveness, we encourage further research in several areas including:

- How are ERP control functions affected by option choices made during installation?
- How can management balance the trade-off between the technology complexity of control activities and business process risks?
- How do changes in technology impact usage of the revised *Framework*?

EXHIBIT 2

Research Opportunities Identified from Review of the Updated COSO *Framework*

Panel A: Overall *Framework*

Integrate Technology Issues

How are ERP control functions affected by option choices made during installation?

How can management balance the trade-off between the technology complexity of control activities and business process risks?

How do changes in technology impact usage of revised *Framework*?

Control Framework Effectiveness

Are control frameworks effective?

To what extent do auditors use COSO, COBIT, both frameworks, or different frameworks?

Are some frameworks more effective for certain purposes?

Will the revised *Framework* improve categorization of IT weaknesses for external financial reporting purposes?

Is the revised *Framework* easier to use, specifically at the entity, division, and/or functional level?

Consider Supply Chain Partner Relationships

What are the risks of the inter-organizational information systems deployed across participants in supply chains?

What controls exist (or should be developed) to reduce inter-organizational information systems risks?

What are the risks and related controls when ERP systems are linked within the supply chain or extended beyond individual enterprises in supply chains?

What are the risks and possible controls available in the technologies that make supply chain partners' systems interoperable?

Use of Principles- versus Rules-Based Approach

Is a principles-based or rules-based approach more suitable for the regulatory task of issuing internal control guidelines?

Is the construction of a true principles-based regulatory regime for internal control evaluation desirable or even possible?

Do the *Framework*'s 17 explicitly described principles, supported by numerous attributes, constitute a *de facto* set of rules?

Under what conditions might an organization fall victim to the Schwarcz (2009) paradox and comply with inferred, but inappropriate, rules regarding the design or implementation of internal controls?

Panel B: Control Environment

Outsourcing Considerations

How can the board of directors effectively oversee outsourced operations?

To what extent is the board of directors involved in negotiations with a service provider?

Are board members truly able to comprehend the complexities of outsourcing relationships, the internal control risks, and mechanisms to address these risks?

Can board members recognize when proposed outsourcing creates personal incentives for corporate executives that might have long-term, adverse consequences for the organization?

After an outsourcing relationship commences, what oversight does the board of directors provide going forward?

How effective is the audit committee in addressing potential risks associated with outsourcing?

(continued on next page)

EXHIBIT 2 (continued)

Linkage between Performance Measures in Control Environment and Achieving Controls in Control Activities

How do organizations currently link tone at the top to specific control activities?

How can this linkage of tone at the top to specific control activities be improved?

How can information processing systems support organizational strategy?

What organizational characteristics influence the combination of results, action, personnel, and cultural controls necessary to achieve optimal organizational success? To achieve specific objectives?

What is the extent to which extrinsic incentives induce behaviors inefficient or harmful to the organization?

To what extent do varying types of controls produce incentives conducive with or contrary to those activities necessary to achieve strategic goals (such as creativity or appropriate levels of risk taking)?

How can information systems be designed and managed to achieve the goals of boundary and diagnostic systems while providing flexibility to adjust to the dynamic business world of today?

How can the AIS literature on controls over dysfunctional behavior and the MA literature on motivators for productive behaviors blend to inform our academic and practitioner communities?

Performance Evaluation and Reward Issues

How effective are 360-degree reports?

Panel C: Risk Assessment

Is the *Framework* missing any critical attributes?

Does listing these attributes in detail result in organizations limiting their objectives to these and not include others more relevant to their particular business strategy?

Panel D: Monitoring Activities

Integrate Continuous Monitoring and Continuous Auditing

What audit procedures should be automated?

What evaluation benchmarks should be used for continuous auditing?

How can data analytics be used to analyze internal controls, transactions, and account balances?

Can continuous auditing be used as an audit-by-exception technique?

Monitoring Outsourced Operations

How often do organizations conduct EDP audits, compliance audits, and other reviews?

Does the frequency of these audits correspond to the effectiveness of internal controls relating to service providers?

What causes controls to evolve over the life of a service audit contract? Audit results? Disclosure of system changes by the service provider? Other factors?

How do organizations implement monitoring systems?

To what extent is monitoring a function of built-in IT controls rather than other audit procedures such as inquiry, documentation, and observation?

(continued on next page)

Overall Framework *Issue 2: Are Control Frameworks Effective?*

Since its passage, SOX has created significant changes in the accounting profession and provided fertile ground for accounting research (Ge and McVay 2005; Haislip et al. 2012; Hunton et al. 2008; Li et al. 2012; Murthy and Reck 2012; Stefaniak et al. 2012; Wolfe et al. 2009). One notable omission in this growing body of work is any examination of how effective these frameworks are in assessing internal control. Although control frameworks

EXHIBIT 2 (continued)

Use of Service Auditor Reports to Monitor Outsourced Operations

To what extent are users of service auditor reports able to identify whether the assertions addressed in the report fully correspond with their organization's relevant financial statement assertions?

How effective are audit committees in addressing important internal control issues related to service providers?

To what extent does management, the board of directors, and the audit committee rely on service audit reports—do they take them at face value or dig deeper?

When service auditors report only on internal controls related to financial reporting, how does management evaluate and monitor controls related to compliance with applicable laws and regulations, and the effectiveness and efficiency of their operations? Is this task delegated to internal audit?

How do organizations deal with complex audit situations resulting from issues such as reliance on multiple service auditor reports and subservice audit reports?

Importance of Internal Control Documentation

Should internal controls be documented?

Is a verbal description of controls as useful in risk assessment or control evaluation as a written narrative or graphical documentation?

Can trust substitute for documentation, and if so, in what contexts is this effective?

Does the personal preparation of documentation, prior to using it to evaluate controls, provide incremental benefit to the effectiveness of how one evaluates the internal controls?

---

were generally employed prior to SOX, the PCAOB (2007a) requirement mandating the use of a framework creates an opportunity for academic researchers to examine the effectiveness of such frameworks.

Recent research explores the effectiveness of the Control Objectives for Information and related Technology (COBIT) framework. By superimposing COBIT's conceptual model onto audit-relevant assessments made by highly experienced IT auditors, Tuttle and Vandervelde (2007) confirm the internal consistency among the underlying constructs of COBIT. In addition, they find COBIT's conceptual model predicts auditors' behavior in the field related to seeking and giving help, as evidenced by postings to a general IT audit listserv.

Research opportunities related to the effectiveness of control frameworks. Opportunities for additional research on the effectiveness of control frameworks include:

- Is the revised *Framework* effective?
- To what extent do auditors use COSO, COBIT, both frameworks, or other frameworks?
- Are some frameworks more effective for specific purposes such as SOX compliance, risk assessment, fraud detection, and/or merger and acquisition work?
- Will the revised *Framework* improve IT weakness categorization for external financial reporting purposes?
- Is the *Framework* easier to use (specifically at the entity, division, and/or functional level)?

Overall Framework *Issue 3: Supply Chain Partner Relationships and Internal Control*

Many organizations undertake activities that are highly dependent on their supply chain partners (Klein and Rai 2009; McFarland et al. 2008). The *Framework* mentions general concerns related to the existence of a supply chain (COSO 2011, 29, 69, 102); however, we encouraged COSO to recognize supply chain relationships more explicitly. For example, the *Framework* articulates a Risk Assessment principle that encourages the organization to identify "risks to the achievement of its objectives across the entity" (COSO 2011, 11). Many supply chain partnerships extend the organization's exposure to risk beyond the entity itself, but the *Framework* does not explicitly address risks originating in supply chain partner activities that exist outside the entity. An organization's dependence on tightly linked supply chain partners could affect its risk (Jaeger 2010) and thus have an impact on its risk assessment process (COSO 2011, 59), control activities (COSO 2011, 77, 86), and the information and communication internal control components (COSO 2011, 94).

We encouraged COSO to consider explicitly the role technology plays in enforcing internal controls on information flows among supply chain partners because information security is implicit in the requirements of SOX (Anand 2008; Damianides 2005). For example, a specific control issue might arise regarding the security of messages moving between supply chain members. Vasarhelyi et al. (2004) note supply chain partners often establish formal communication agreements among trading partners including specific security and privacy protocols to follow. For example, requiring an encryption system in such an agreement would create an additional protection layer, adding to the strength of internal control. Other specific technologies, such as firewalls, intrusion prevention, and intrusion detection, could be employed to increase the level of internal control achieved (Wallace et al. 2011). Controls designed to meet specific inter-organizational objectives in an electronic data interchange (EDI) environment would be helpful since EDI's benefits depend on using appropriate controls to mitigate specific risks inherent in the technology (Grabski et al. 2011; Lee et al. 2005).

Grabski et al. (2011) observe that supply chain partners create inter-organizational information systems by linking their individual ERP systems using component engineering tools such as CORBA and JavaBeans, middleware products, and platform-independent communication protocols such as XML, XBRL, and HTML. Vathanophas (2007) found a lack of consensus on critical success factors among developers of inter-organizational and extended-enterprise information systems. The variety of technologies used to develop these systems, combined with a lack of agreement on critical success factors, suggests specific internal control guidance is important.

Research opportunities related to supply chain partner relationships. To summarize, the following research opportunities relate to supply chain partner relationships:

- What are the risks of the inter-organizational information systems deployed across participants in supply chains?
- What controls exist (or should be developed) to reduce inter-organizational information systems risks?
- What are the risks and related controls when ERP systems are linked within the supply chain or extended beyond individual enterprises in supply chains?
- What are the risks and possible controls available in the technologies used to facilitate supply chain partners' systems interoperability, including security over data transmission and privacy implications?

Overall **Framework** ***Issue 4: Use of a Principles- versus Rules-Based Approach***

One stated goal of the *Framework* is to move toward a principles-based approach to the evaluation of internal control. Specifically, the revised *Framework* states that its principles, together with their supporting attributes, form "the criteria that will assist management in assessing whether an entity has effective internal control" (COSO 2011, 140). The *Framework* does not discuss the reasons for this change in its approach. Further, the *Framework* does not appear to be informed by the substantial body of existing research on: (1) how to determine whether a specific regulatory regime is principles based or rules based, and (2) which approach is most appropriate to use in a particular setting (e.g., Bentson et al. 2006; Black 2010; Cunningham 2007; Ford 2008, 2010;

Kershaw 2005; Ojo 2010, 2011; Schwarcz 2009). A key finding in this literature is that few, if any, examples of pure rules-based or principles-based regulatory regimes exist. For example, Black (2010) and Ford (2008, 2010) argue that virtually all such guidelines and regulations are a mixture of both approaches.

Bentson et al. (2006) evaluated Financial Accounting Standards Board (FASB) rules-based standards and found the format of the standards and their contents to be interdependent. For example, an accounting principle that requires substantial judgment will also require significant guidance and even exceptions; this can result in a principle that operates very much as a set of rules. They conclude that the international move toward principles-based accounting standards might be doomed to end in a regime that is called principles based but in fact operates much as a rules-based regime would. Cunningham (2007) presents similar arguments, noting the term "principles based" is misleading because construction of such regulatory schemes is impossible. The *Framework* includes 17 explicitly described principles, each supported by a number of attributes (COSO 2011, 140). Future research could examine the *Framework* to determine whether the specific guidance in this collection of principles and clarifying attributes constitutes a set of rules.

Researchers could consider whether the evaluation of internal control is a polycentric process (Black 2010) because multiple stakeholders (managers, internal audit staff, and independent auditors) and regulators (SEC and other government agencies, guidance creators such as COSO and the IT Governance Institute) exist. Black's (2010) taxonomy could provide a structure for researchers evaluating whether a principles-based regime is the most appropriate for internal control evaluation.

Schwarcz (2009) identifies an interesting paradox in the implementation of principles-based regulatory schemes. He notes that unless an organization subject to a principles-based regime is protected from liability, it will act as if subject to a rule, perhaps even an unintended rule. Since organizations subject to the *Framework* are not insulated from liability, this research suggests an unintended consequence of using a principles-based approach in the *Framework* could be organizations inferring inappropriate rules and then following them.

Research opportunities related to the use of a principles- versus rules-based approach. The *Framework*'s omission of any discussion regarding the relative merits of principles-based and rules-based regulatory regimes prompts several potential research questions. These include:

- Is a principles-based or rules-based approach more suitable for the regulatory task of issuing internal control guidelines?
- Is the construction of a true principles-based regulatory regime for internal control evaluation desirable or even possible?
- Do the *Framework*'s 17 explicitly described principles, supported by numerous attributes, constitute a *de facto* set of rules?
- Under what conditions might an organization fall victim to the Schwarcz (2009) paradox and comply with inferred, but inappropriate, rules regarding the design or implementation of internal controls?

Control Environment

We noted three areas of concern related to the control environment. We first discuss concerns regarding the lack of consideration of the implications of outsourcing. Second, we examine the linkage between performance measures in the Control Environment principle and achieving controls in the control activities. Finally, we consider performance evaluation and reward issues.

Control Environment Issue 1: Consider the Implications of Outsourcing

In today's business environment, organizations often outsource specific systems such as technology, human resources, and payroll. In these arrangements, organizations send information to the outsourcer (service provider), who processes the information and provides information back to the organization. Although the revised *Framework* recognizes the added risks and challenges associated with outsourcing (e.g., COSO 2011, 19), it states the "*Framework* can be applied to the entire entity regardless of what choices management makes about how it will execute business activities that support its objectives, either directly or through external relationships" (COSO 2011, 19). However, the *Framework* provides little specific guidance on how to address the impact of outsourcing on an organization's internal control structure.

The control environment is the *Framework* component most affected by outsourcing and thus likely ineffective in these arrangements. Although an organization can set the tone at the top and communicate expectations through written mission statements, codes of conduct, etc. (e.g., COSO 2011, 27–30, 67, 97), service provider employees are more likely to be influenced by the tone set by their own entity, and this tone might differ considerably from the outsourcing organization's tone. Further, although expectations might be included in contracts with service providers (COSO 2011, 30, 37, 113), how can an organization know if these expectations and the tone at the top actually trickle down through the service provider's organizational structure? Service providers are often located in other countries, and bring different cultural norms and business practices (COSO 2011, 29) into the mix of factors affecting the behavior of service provider employees. In fact, it can be difficult for an organization's employees to manage or collaborate with personnel from a different culture, and also difficult for service provider employees working in positions requiring intensive interaction with customers and U.S. employees such as call center and technical support activities (Lewin and Peeters 2006). Although the *Framework* briefly acknowledges some of these concerns and states management is still responsible for the performance of processes delegated to service providers (COSO 2011, 29, 38, 131), more specific guidance on how to meet these responsibilities is needed.

Prior research demonstrates the difficulty of altering the behavior of service provider employees through conventional control environment mechanisms. For example, service providers can struggle to abide by the many different individual codes of conduct used by their client organizations (Jorgensen et al. 2003, as cited in Antonio 2011). Service providers' use of corporate codes of conduct can also be ineffective because such codes are not widely recognized in developing countries, many service providers have an existing practice of failing to comply with legal requirements, compliance with codes of conduct does not improve a supplier's social and environmental performance, and auditing a service provider's compliance with a code of conduct is ineffective (Lund-Thomsen 2008; Boyd et al. 2007). Antonio (2011) also notes compliance might worsen the working conditions of service provider employees. For example, codes of conduct might limit the number of hours and days in a work week, yet workers in developing countries often need to work the extra hours and days to provide for their families. When companies pressure service providers to comply with organizational policies, motivation to comply is lessened and cheating can result (Baden et al. 2009).

In a similar fashion, Lund-Thomsen (2008) argues that codes of conduct might do more harm than good. Academics and policymakers often fail to consider the realities faced by many developing country suppliers, workers, and communities. Many cultures (e.g., Latin American, Asian, and African) believe businesses have social obligations to employees and society that are not well captured by codes of conduct (Lund-Thomsen 2008). For these reasons, when organizations develop codes of conduct to be used by service providers in these cultures, they must include the voices of suppliers, workers, and communities in the design, implementation, monitoring, and impact assessment (Lund-Thomsen 2008). Further, cultural clashes between an organization and a service provider occur on two levels: (1) corporate cultures with different norms in terms of speed, style, decision making, and organizational structure; and (2) national/regional cultures with subtle differences in verbal, non-verbal, and written communications (McCray 2008). In addition, there might be cultural expectation differences, including the acceptable level of open debate, acknowledgement of potential problems, and willingness to deviate from normal processes to get the work done (McCray 2008).

Further, an effective control environment is characterized by a board of directors collectively having the skills and expertise needed for proper oversight, including knowledge of critical systems and technology challenges and opportunities (COSO 2011, 33–35). We question whether board members, either individually or collectively, possess the expertise to fully understand the complexity of an internal control system that extends outside the organization to include its service providers. In addition, the decision to outsource is often linked to factors such as CEO compensation structure (see Blaskovich and Mintchik [2011] for an extensive review of key determinants of outsourcing decisions), making the board of directors' oversight responsibilities considerably more difficult.

The Commitment to Competence principle charges human resources with the responsibilities to attract, train, mentor, evaluate, and retain employees (COSO 2011, 40), and charges management with the responsibility to evaluate the competence of outsourced service providers (COSO 2011, 40). This principle can lose its effectiveness in outsourced operations when organizations attempt to achieve contradictory objectives such as cost reduction per customer transaction and quality-oriented customer service (D'Cruz and Noronha 2012). In fact, Lewin and Peeters (2006) report cost reduction and improved service levels among the top reasons corporations decide to outsource; however, poor service quality and service center employee turnover are two of the top problems actually encountered. In many organizations, an outsourcing process in which savings are largely derived from reduced labor costs is at odds with a commitment to competence.[3]

Research opportunities related to the implications of outsourcing. Our discussion suggests several research opportunities including:

- How can the board of directors effectively oversee outsourced operations?
- To what extent is the board of directors involved in negotiations with a service provider?
- Are board members truly able to comprehend the complexities of outsourcing relationships, the internal control risks, and mechanisms to address these risks?
- Can board members recognize when proposed outsourcing creates personal incentives for corporate executives that might have long-term, adverse consequences for the organization?
- After an outsourcing relationship commences, what oversight does the board of directors provide going forward?
- How effective is the audit committee in addressing potential risks associated with outsourcing?

Control Environment Issue 2: Linkage of Performance Measures in Control Environment and Achieving Controls in Control Activities

The fifth Control Environment principle asserts the organization should hold individuals accountable for their internal control responsibilities. Further, the *Framework* recognizes "incentives drive behavior" (COSO 2011, 44) and nonfinancial rewards can be effective, positive

[3] As noted, numerous risks and problems associated with outsourcing reduce the effectiveness of the control environment. Thus, effective monitoring of these activities is important. However, monitoring outsourced activities presents its own set of challenges. We discuss these challenges in the Monitoring Activities section.

incentives; thus it encourages managers to review "the organization's measurement and reward structures to ensure that they do not create incentives for inappropriate conduct" (COSO 2011, 44). However, it is not clear how this Control Environment principle is translated to the individual control process level or how these reward-focused activities can enhance control procedure compliance. Essentially, there is disconnect between the high-level discussion of "tone at the top" and the more detailed and specific control activities where policies are established for application or general level controls. We believe more thought is needed in linking performance measures from management control systems, discussed in the control environment, with the achievement of controls discussed in control activities, particularly in regard to the reward and punishment of control-related employee performance as well as available mechanisms to focus employee attention on uncompensated, yet important control activities.

There is a similar disconnect in the academic literature, given the differing perspectives on internal control by managerial accounting (MA) and accounting information systems (AIS) researchers. Although MA considers incentives and performance evaluation systems as their primary means of achieving organizational control, AIS focuses more on the procedures designed into manual and computerized information systems.

The *Framework* includes both types of control, addressing performance evaluation systems within the Control Environment component and information system procedures in the Control Activities component. Controls explored by MA researchers tend to focus on motivating managers to align their goals with those of the organization and adopt an appropriate level of risk so the organization can achieve its strategic objectives. However, the vast majority of internal control research in the AIS and auditing literature centers on the operational level of control, as described in control activities, where data accuracy and validity are the primary concerns.

To further this discussion, we describe two theoretical frameworks for use in future research. The first is based upon objects of control, and aligns the interests of ownership and employees, as well as facilitates the implementation of effective performance evaluation systems. The second seeks to combine operational and strategic control elements to demonstrate how organizations can achieve a meaningful balance.

Merchant and Van der Stede (2007) identify four categories of management control systems: results, action, personnel, and cultural controls. Controls in all of these categories are designed to increase the likelihood employees will act in the organization's best interests. Results controls involve rewarding employees for achieving targets or outcomes. Because affected employees must have the ability to influence the selected measure(s) of interest for their results controls to be effective, careful thought should be given prior to implementation of results controls. Action controls focus on rules, policies, and procedures, and attempt to ensure employees engage or do not engage in certain behaviors. All organizations use action controls to some degree, but the scope of usage will depend upon the extent to which employee behavior must be constrained and/or monitored.

Personnel controls operate on the premise that employees often demonstrate self-monitoring and self-motivation. In this domain, emphasis is on maintaining a quality workforce, and providing employees with the resources and information they need to perform their roles effectively and independently. Cultural controls promote mutual monitoring among coworkers. In a strong organizational culture, employees tend to take ownership and adhere to a set of organizational norms and values, and expect their coworkers to follow these same principles, and place peer pressure on those who violate the norms. Each type of control serves a different purpose; thus, combinations of controls in two or more areas may provide the most effective foundation for a given control issue within each unique organization. For researchers, this framework may provide theoretical support for bridging the MA and AIS research literatures.

Our second theoretical framework, Simons' (1995) theory of Levers of Control, provides another basis for combining the disparate streams of research from the AIS and MA literatures.

Simons argues this historical divide in focus occurred because researchers were caught in old philosophies of control and management. Simons (1995) asserts organizations can achieve a balance that gives managers both empowerment and accountability. Simons' framework for controlling business strategy includes four variables: (1) belief systems or core values that inspire and direct the search for new opportunities; (2) boundary systems that limit opportunity-seeking behavior, thus protecting the organization from risks to be avoided; (3) interactive control systems that stimulate the emergence of new ideas and strategies in the face of uncertainty; and (4) diagnostic control systems or critical performance variables used to motivate, monitor, and reward achievement of specified goals. In this framework, interactive control systems and belief systems create inspirational forces, while boundary systems and diagnostic systems create constraints.

One of Simons' concerns is that managers focus primarily on incentives and pay too little attention to diagnostic systems, perhaps because the design of systems to monitor critical performance variables is seldom dynamic enough to ensure control targets are appropriate for the risks created by the organization's current strategy. Because "what you measure is what you get," monitoring focused on out-of-date performance variables will lead to effort expended on non-productive activities (Simons 1995, 81). Chow et al. (1995) suggest the joint impact of monitoring and incentives should be examined since the two organizational control mechanisms are intertwined, and empirical researchers are beginning to bridge this gap between the MA and AIS perspectives on control. Both of the frameworks described here offer a basis on which to achieve this integration. For example, Christ et al. (2012) examine whether organizations can effectively use internal controls to complement incentive compensation in aligning employee behavior with goals in a multidimensional task. They find overall employee performance on a multidimensional task can be higher when organizations compensate employees on one dimension and control them on the other dimension, than when organizations compensate both dimensions.

Hunton et al. (2008) explore one way to combine the AIS and MA literatures by varying performance evaluation time horizon (short versus long) and type of monitoring (continuous versus periodic), and noting the associated effects on both functional and dysfunctional aspects of managerial decisions. This research supports the notion that operational-level control activities (such as continuous monitoring) can negatively impact strategic objectives.

Research opportunities related to the linkage of performance evaluation in control environment and achieving controls in control activities. Several research opportunities relate to the linkage of performance evaluation in control environment and achieving controls in control activities including:

- How do organizations currently link tone at the top to specific control activities?
- How can this linkage of tone at the top to specific control activities be improved?
- How can information processing systems support organizational strategy?
- What organizational characteristics influence the combination of results, action, personnel, and cultural controls necessary to achieve optimal organizational success and to achieve specific objectives?
- What is the extent to which extrinsic incentives induce behaviors inefficient or harmful to the organization?
- To what extent do varying types of controls produce incentives conducive with or contrary to those activities necessary to achieve strategic goals (such as creativity or appropriate levels of risk taking)?
- How can information systems be designed and managed to achieve the goals of boundary and diagnostic systems while providing flexibility to adjust to the dynamic business world of today?

- How can the AIS literature on controls over dysfunctional behavior and the MA literature on motivators for productive behaviors blend to inform our academic and practitioner communities?[4]

Control Environment Issue 3: Performance Evaluation and Reward

The *Framework* states performance objectives and rewards cascade down through the organization (COSO 2011, 46), and management, the board of directors, and other personnel evaluate performance periodically at each level (COSO 2011, 44, 46). Performance evaluation should also flow upward in an organization to reveal breakdowns in the internal control system at specific levels. For example, subordinates might reveal problems and attitudes their supervisors have concealed from upper management. One way to accomplish this upward flow is by using 360-degree reports, in which individuals evaluate those above and below them in the organizational hierarchy.

Research opportunities related to performance evaluation and reward. Our discussion generates the following research opportunity:

- How effective are 360-degree reports?

Risk Assessment

We did not make specific recommendations to COSO regarding the Risk Assessment component. However, we did identify relevant research opportunities.

Research opportunities related to risk assessment. We note the *Framework* suggests the organization specify relevant objectives with sufficient clarity to enable the identification and assessment of risks relating to the objectives. Further the *Framework* presents a set of attributes related to each objective category (COSO 2011, 71–74). Research could examine:

- Is the *Framework* missing any critical attributes?
- Does listing these attributes in detail result in organizations limiting their objectives to these and not including others more relevant to their particular business strategy?

Monitoring Activities

In this section we discuss four concerns related to monitoring activities. Our first concern is the need to better incorporate continuous monitoring and continuous auditing into the *Framework*. Next, we discuss monitoring issues arising from a dependence on service providers for outsourced operations. Third, we discuss the use of service auditor reports as a means of monitoring outsourced operations. This section concludes with a discussion of the importance of documenting internal controls.

Monitoring Activities Issue 1: Better Incorporate Continuous Monitoring/Continuous Auditing into the Framework

The jointly sponsored CICA/AICPA Continuous Auditing project stipulates the development of the digital economy has created a demand from decision makers, such as potential investors and creditors, for more timely assurance on a number of information topics extending well beyond traditional financial statements (CICA 1999). The authors argue, if decision makers require a more continuous information stream, they will also demand independent assurances about its reliability. Consequently, a greater need for real-time auditing emerges. However, the *Framework* does not

[4] Libby and Seybert's (2009) examination of the effects of regulation on earnings management and accounting choice could serve as a source of specific research questions.

address continuous auditing and monitoring practices explicitly. The *Framework* addresses technology itself in a general and perhaps overly broad level (COSO 2011, 95–99).

We define *continuous auditing* as "any method used to perform audit-related activities on a more continuous or continual basis" and *continuous monitoring* as "a process that management puts in place to ensure that its policies, procedures, and business processes are operating effectively" (IIA 2005, 1). Continuous auditing has the ability to monitor all relevant business activities on a continual basis and allow for real-time assurances relative to controls and financial information. Internal audit staffs might use continuous auditing to: (1) provide evidence controls are operating as intended, (2) repeat computer operations tests, and (3) perform queries to verify controls are functioning properly (Vasarhelyi et al. 2004, 19). We noted the *Framework* includes no discussion of how continuous auditing by internal audit staffs can improve internal controls, and we recommended that COSO add this discussion to the document.

Although continuous auditing involves independent auditors in the provision of various assurance services, continuous monitoring requires management implementation of specific monitoring routines. Continuous auditing examines all relevant business activities continually and allows for real-time assurances regarding controls, transactions, and information; continuous monitoring does not. Despite their name, continuous monitoring programs do not operate continuously. Instead, they are activated on a periodic basis (e.g., weekly, monthly), and thus produce information from historical data in a batch processing mode. Additionally, continuous monitoring often refers to tools and methods used for smaller scale monitoring of high-risk subsets of business transactions. Glover et al. (2000) describe automated tools used for continuous monitoring.

Research opportunities related to incorporating continuous monitoring/continuous auditing. Chan and Vasarhelyi (2011) propose a four-stage continuous audit paradigm intended to facilitate research on continuous auditing. They propose research into:

- What audit procedures should be automated?
- What evaluation benchmarks should be used for continuous auditing?
- How can data analytics be used to analyze internal controls, transactions, and account balances?
- Can continuous auditing be used as an audit by exception technique?

Monitoring Activities Issue 2: Monitoring Outsourced Operations[5]

Outsourcing creates a specific risk not currently addressed by the *Framework*. Management makes the strategic decision to outsource because it believes the benefits (often cost savings) outweigh the risks (COSO 2011, 19). However, these cost savings might lead to a dependence on a service provider, subject to other factors such as the availability of alternative service providers and the ease of changing to another provider. These factors might not be adequately addressed in management's succession plan (COSO 2011, 42). Given this dependency, management might be unable to enforce contractual terms, including required standards of conduct, right-to-audit clauses, etc., or simply might be inclined to overlook problems to maintain a good relationship with the provider (COSO 2011, 102).

Opportunistic behavior on the part of the service provider occurs when there are a limited number of viable service providers, high switching costs for the organization, and asset specificity as a result of investing in assets whose use is limited to the outsourced activities (Sullivan and

[5] Earlier, we discussed how outsourcing operations might reduce the effectiveness of the control environment and noted the need for monitoring outsourced operations. In this section, we discuss the nature of the organization-service provider relationship and the monitoring problems that result from these relationships.

Ngwenyama 2005). In these situations, management might need to employ external third-party monitoring and construct contracts containing incentives (penalties) for good (poor) performance (Bryson and Sullivan 2003; Ngwenyama and Bryson 1999). However, some research indicates the use of mediated power (i.e., extrinsic motivation induced by the use of reward, coercive, or legal forms of power) decreases the service provider's satisfaction with and commitment to the relationship, and increases the potential for opportunistic behavior (Handley and Benton 2012). Further, the difficulty of switching providers and the expected level of supply market consolidation are negatively associated with the use of mediated power, whereas contract management difficulty is positively associated with such use (Handley and Benton 2012). In sum, incentive contracts might not always be effective in reducing opportunistic behavior, thus increasing the importance of monitoring in some situations.

The *Framework* recognizes both separate and ongoing evaluations might be needed for higher priority risks (COSO 2011, 110–111). Further, separate evaluations might be conducted by either internal or external parties (COSO 2011, 101–102, 109, 112–113). Indeed, monitoring is well established as a means of reducing risks associated with information asymmetry in principal-agent relationships (Jensen and Meckling 1976). However, monitoring outsourced operations presents numerous challenges. Multiple service providers might need to be monitored (Miller 2009). Additionally, although major effort is expended when creating contracts and getting projects started, organizations often put fewer resources into ongoing monitoring activities. This contributes to the high failure rates of outsourcing projects; 20 percent fail within the first two years and 50 percent fail within five years (Miller 2009).

Adding to these challenges is the difficulty of negotiating audit rights within the contract. Service providers typically do not want customers to have access to system configuration parameters because these are regarded as trade secrets and competitive advantages (Jorgensen 1996). Additionally, service providers must implement controls that separate and secure each customer's data so they are reluctant to grant internal auditors full data access (Jorgensen 1996).Thus, internal auditors must know in advance the types of data access needed so these specific audit rights can be written into the contract. This will include, at a minimum, complete access to their own organization's program files and the data center's system support tools; rights to conduct a general IT controls review of the service provider's data centers; and reviews for contract compliance, billing, and efficiency (Jorgensen 1996).

Manning et al. (2011) recognize service providers sometimes allow for organizational involvement to increase the likelihood of contract renewal. Organizational involvement increases joint equity in the relationship, and creates the much-desired opportunity for monitoring and control for the organization (Manning et al. 2011). The downside, however, is the possibility the interaction between employees of the service provider and the organization can lead to discussions about wages and other working conditions that are usually worse in the service provider firm (Manning et al. 2011). Thus, involvement might not always be an easy solution to the agency problems associated with outsourcing.

Research opportunities related to monitoring service providers. Monitoring is an important part of the internal control framework of an organization, especially in regard to service provider contracts. Research opportunities in this area include:

- How often do organizations conduct EDP audits, compliance audits, and other reviews?
- Does the frequency of these audits correspond to the effectiveness of internal controls relating to service providers?
- What causes controls to evolve over the life of the service audit contract? Perhaps disclosure of system changes by the service provider?
- How do organizations implement monitoring systems?

- To what extent is monitoring a function of built-in IT controls versus other audit procedures such as inquiry, documentation, and observation?

Monitoring Activities Issue 3: Service Auditor Reports

The *Framework* should address the risk of overreliance on service provider audit reports. Although the *Framework* states organizations should consider the content of assertions and attestations satisfied when reviewing an independent audit or examination report (COSO 2011, 113), we recommended to COSO the *Framework* state clearly that service auditor reports might be intended to satisfy the needs of several different user auditors, and thus might not provide evidence relevant to significant assertions in the organization's financial statements. In these situations, material weaknesses in internal control might be overlooked due to an overreliance on the service auditor's report without in-depth separate evaluations conducted within the service provider organization for the unaddressed, yet significant, relevant assertions. Further, even when the service auditor's report addresses all significant, relevant assertions, annual reports might not be sufficient for areas of high risk, and organizations might need to consider supplementing annual reports with additional and more frequent evaluations, including agreed-upon procedure engagements.

Service auditor reports might only include objectives related to financial reporting. In such instances, management needs additional evaluations to insure controls at the service provider relating to the organization's compliance with applicable laws and regulations, as well as the effectiveness and efficiency of their operations. Service auditors may report on either (1) the design and implementation of controls as of a specified date; or (2) the design, implementation, and operating effectiveness of controls over a specified period of time (AICPA 2011). The period of time covered by a service auditor's tests of operating effectiveness of controls (minimum of six months) might not coincide with or provide the complete coverage needed by the organization. Although service auditors are required to inquire about changes during the period of time covered by their audit (AICPA 2011), inquiry might not be sufficient to reveal changes creating deficiencies.

Service providers can outsource some of their own services, referred to as subservice providers (AICPA 2011). In these instances, the scope of a service auditor's examination might or might not extend to controls of the subservice provider, thus increasing audit complexity and perhaps limiting the usefulness of audit reports. Further, service provider management furnishes the service auditor a description of the system, the assertions to be tested, the criteria to be used, a description of the control objectives, and the identified risks of not achieving those objectives (AICPA 2011). Organizations need to be sure their own assertions and objectives are included in the specifications provided by the service provider's management. Also, a service provider's controls might include necessary complementary controls at the user organization. Organizations should be careful not to overlook their responsibility for these controls.

Recent audit deficiencies noted by the PCAOB discuss these concerns:

> The inspection teams observed deficiencies related to firms' reliance on controls over the information provided by service organizations as well as firms' use of information produced or processed by service organizations. These deficiencies included the failure (a) to perform any of the procedures listed in the preceding paragraph,[6] or to test the reports or data, when relying on reports produced or data processed by service organizations, (b) to assess the operating effectiveness of the user controls identified in the service auditor's

[6] These procedures include: (1) test the issuer's controls (user controls) over the activities of the service organization, (2) obtain a service auditor's report on the operating effectiveness of controls placed in operation at the service organization or a report on the application of agreed-upon procedures that describes the relevant tests of controls, or (3) test controls at the service organization (PCAOB 2007b, 13).

> report as necessary to rely on the controls over the information processed by the service organization, or (c) to obtain evidence about the operating effectiveness of controls placed in operation at the service organization when the service auditor's report did not address the operating effectiveness of the controls. The deficiencies also included instances where firms relied on controls at service organizations and obtained service auditors' reports on those controls, but those reports did not cover a significant portion of the period of reliance and the firms failed to perform procedures regarding the service organizations' controls during the period not covered by the reports. (PCAOB 2007b, 13)

Research opportunities related to overreliance on service auditor reports. We were unable to identify any academic research related to reliance on service auditor reports, yet it appears overreliance might be a serious problem. Numerous research opportunities exist, including:

- To what extent are users of service auditor reports able to identify whether the assertions addressed in the report fully correspond with their organization's relevant financial statement assertions?
- How effective are audit committees in addressing important internal control issues related to service providers?
- To what extent does management, the board of directors, and the audit committee rely on service audit reports—do they take them at face value or dig deeper?
- When service auditors report only on internal controls related to financial reporting, how does management evaluate and monitor controls related to compliance with applicable laws and regulations, and the effectiveness and efficiency of their operations? Is this task delegated to internal audit?
- How do organizations deal with complex audit situations resulting from issues such as reliance on multiple service auditor reports and subservice audit reports?

Monitoring Activities Issue 4: Should Internal Controls Be Documented?

The proposed *Framework* states, "There may be instances where internal controls are informal and undocumented" (COSO 2011, 24). Further, it states, "When considering circumstances such as the nature and scope of information transferred between parties and the nature of the processing and reporting the outsourced service provider performs, an entity may be able to determine that there is sufficient internal control over processing provided by the outsourced service provider without additional documentation" (COSO 2011, 113). We recommended COSO reconsider these assertions because we believe it is difficult to gather and evaluate evidence on the design and operational effectiveness of a control without documentation of the control itself. Moreover, the auditing of undocumented controls would prove difficult, at best, without information regarding the control.

In formulating our recommendation to COSO, we found a number of research studies explaining the benefits of various types of documentation (cf. Bierstaker et al. 2009; Boritz and Borthick 2012), as well as field studies identifying the types of documentation currently employed in practice (cf. Bradford et al. 2007) and cases to assist in the training of documentation preparation (cf. Borthick et al. 2010; Curtis and Borthick 1999). However, we found no research evaluating whether controls actually needed to be documented.

Research opportunities related to internal control documentation. Several possible research opportunities exist, including:

- Should internal controls be documented?
- Is verbal description of controls as useful in risk assessment or control evaluation as written narrative or other forms of documentation?

- What is the role of trust in internal control assessment? That is, can trust substitute for documentation, and if so, in what contexts is this effective?
- Does the personal preparation of documentation, prior to using it to evaluate controls, provide incremental benefit to the effectiveness of how one evaluates internal controls?

V. DISCUSSION AND CONCLUSION

Given significant changes in the business environment and technology advancements, COSO recently issued an exposure draft updating its 1992 internal control framework. In this paper we examined the proposed changes to the COSO framework, offered suggestions to improve the framework, and identified important research opportunities related to the proposed framework.

Our work is important to both accounting information systems researchers and educators. First, the new framework integrates information technology into internal control concepts. This generates several new challenges for academics. Second, we inform accounting information systems educators on important framework changes that will impact their classroom teaching.

We acknowledge several limitations of this work. First, this article reflects the collective opinion of only five members of the American Accounting Association's Information Systems Section. Second, we do not attempt to present a complete literature review of all AIS research related to the COSO framework. Rather, our discussion is guided by the recommendations we provided to the Committee of Sponsoring Organizations for improving their proposed revisions of the framework.

REFERENCES

American Institute of Certified Public Accountants (AICPA). 2006. *Understanding the Entity and Its Environment and Assessing the Risks of Material Misstatement*. Statement on Auditing Standards No. 109. New York, NY: AICPA.

American Institute of Certified Public Accountants (AICPA). 2011. *Reporting on Controls at a Service Organization*. Statement on Standards for Attestation Engagements No. 16. New York, NY: AICPA.

Anand, S. 2008. Information security implications of Sarbanes-Oxley. *Information Security Journal: A Global Perspective* 17 (2): 75–70.

Antonio, K. W. L. 2011. The implementation of social responsibility in purchasing in Hong Kong/Pearl River Delta—A case study. *Strategic Outsourcing: An International Journal* 4 (1): 13–46.

Baden, D. A., I. A. Harwood, and D. G. Woodward. 2009. The effect of buyer pressure on suppliers in SMEs to demonstrate CSR practices: An added incentive or counter productive? *European Management Journal* 27: 429–441.

Bentson, G. J., M. Bromwich, and A. Wagenhofer. 2006. Principles- versus rules-based accounting standards: The FASB's standard setting strategy. *ABACUS* 42 (2): 165–188.

Bierstaker, J. L., J. E. Hunton, and J. C. Thibodeau. 2009. Do client-prepared internal control documentation and business process flowcharts help or hinder an auditor's ability to identify missing controls? *Auditing: A Journal of Practice & Theory* 28 (1): 79–94.

Black, J. 2010. *The Rise, Fall and Fate of Principles Based Regulation*. Working paper, London School of Economics.

Blaskovich, J., and N. Mintchik. 2011. Information technology outsourcing: A taxonomy of prior studies and directions for future research. *Journal of Information Systems* 25 (1): 1–36.

Boritz, E., and A. F. Borthick. 2012. *Does the Type of Business Process Representation Affect Auditors' Ability to Assess Control Risk?* Working paper, University of Waterloo.

Borthick, A. F., G. P. Schneider, and A. O. Vance. 2010. Preparing graphical representations of business processes and making inferences from them. *Issues in Accounting Education* 25 (3): 569–582.

Boyd, D. E., R. E. Spekman, J. W. Kamauff, and P. Werhane. 2007. Corporate social responsibility in global supply chains: A procedural justice perspective. *Long Range Planning* 40: 341–356.

Bradford, M., S. B. Richtermeyer, and D. F. Roberts. 2007. Systems diagramming techniques: An analysis of methods used in accounting education and practice. *Journal of Information Systems* 21 (91): 173–212.

Bryson, K., and W. E. Sullivan. 2003. Designing effective incentive-oriented contracts for application service provider hosting of ERP systems. *Business Process Management Journal* 9 (6): 705–721.

Canadian Institute of Chartered Accountants (CICA). 1999. *Continuous Auditing Research Report*. Toronto, ON: CICA.

Chan, D. Y., and M. A. Vasarhelyi. 2011. Innovation and practice of continuous auditing. *International Journal of Accounting Information Systems* 12 (2): 152–160.

Chow, C. W., M. Hirst, and M. D. Shields. 1995. The effects of pay schemes and probabilistic management audits on subordinate misrepresentation of private information: An experimental investigation in a resource allocation context. *Behavioral Research in Accounting* 7: 1–16.

Christ, M. H., S. A. Emett, W. B. Tayler, and D. A. Wood. 2012. *To Compensate or Control? Motivating Employees in a Multidimensional Task*. Working Paper, The University of Georgia, Cornell University, Emory University, Brigham Young University.

Committee of Sponsoring Organizations of the Treadway Commission (COSO). 2011. *Internal Control—Integrated Framework*. Available at: http://www.coso.org/ic-integratedframework-summary.htm

Cunningham, L. A. 2007. A prescription to retire the rhetoric of "principles-based systems" in corporate law, securities regulation, and accounting. *Vanderbilt Law Review* 60 (5): 1409–1493.

Curtis, M. B., and A. F. Borthick. 1999. Evaluation of internal control from a control objective narrative. *Journal of Information Systems* 13 (1): 63–81.

Damianides, M. 2005. Sarbanes-Oxley and IT governance: New guidance on IT control and compliance. *Information Systems Management* 22 (1): 77–85.

D'Cruz, P., and E. Noronha. 2012. Cornered by conning: Agents' experiences of closure of a call center in India. *The International Journal of Human Resource Management* 23 (5): 1019.

DeFelice, A. 2010. *Cloud Computing: What Accountants Need to Know*. Available at: http://www.journalofaccountancy.com/Issues/2010/Oct/20102519.htm

Dehning, B., and V. J. Richardson. 2002. Returns on investments in information technology: A research synthesis. *Journal of Information Systems* 16 (1): 7–30.

Dehning, B., V. J. Richardson, and R. W. Zmud. 2003. The value relevance of announcements of transformational information technology investments. *MIS Quarterly* 27 (4): 637–656.

Dehning, B., V. J. Richardson, and R. W. Zmud. 2007. The financial performance effects of IT-based supply chain management systems in manufacturing firms. *Journal of Operations Management* 25 (June): 806–824.

Dehning, B., V. J. Richardson, A. Urbaczewski, and J. D. Wells. 2004. Reexamining the value relevance of e-commerce initiatives. *Journal of Management Information Systems* 21 (1): 55–82.

Dehning, B., V. J. Richardson, and T. Stratopoulos. 2005. Information technology investments and firm value. *Information and Management* 42 (7): 989–1008.

Ford, C. 2008. New governance, compliance, and principles-based securities regulation. *American Business Law Journal* 45 (1): 1–60.

Ford, C. 2010. Principles-based securities regulation in the wake of the global financial crisis. *McGill Law Journal* 55 (2): 257–307.

Ge, W., and S. McVay. 2005. The disclosure of material weaknesses in internal control after the Sarbanes-Oxley Act. *Accounting Horizons* 19 (3): 137–158.

Glover, S. M., D. Prawitt, and M. B. Romney. 2000. The software scene. *Internal Auditor* 57 (4): 49–57.

Grabski, S. V., and S. A. Leech. 2007. Complementary controls and ERP implementation success. *International Journal of Accounting Information Systems* 8 (1): 17–39.

Grabski, S. V., S. A. Leech, and P. J. Schmidt. 2011. A review of ERP research: A future agenda for accounting information systems. *Journal of Information Systems* 25 (1): 185–211.

Haislip, J. Z., A. Masli, V. J. Richardson, and J. M. Sanchez. 2012. *The Impact of Information Technology Material Weaknesses on Corporate Governance: Evidence from Executive and Director Turnover, and IT Governance Changes*. Working paper, University of Arkansas.

Handley, S. M., and W. C. Benton, Jr. 2012. Mediated power and outsourcing relationships. *Journal of Operations Management* 30 (3): 253–267.

Henderson, B. C., K. Kobelsky, V. J. Richardson, and R. E. Smith. 2010. The relevance of information technology expenditures. *Journal of Information Systems* 24 (2): 39–77.

Hunton, J. E. 2002. Blending information and communication technology with accounting research. *Accounting Horizons* 16 (1): 55–67.

Hunton, J. E., E. G. Mauldin, and P. Wheeler. 2008. Potential functional and dysfunctional effects of continuous monitoring. *The Accounting Review* 83 (6): 1551–1569.

Institute of Internal Auditors (IIA). 2005. *Continuous Auditing: Implications for Assurance, Monitoring and Risk Assessment*. Global Technology Audit Guide 3. Available at: http://www.theiia.org/guidance/technology/gtag3/

Jaeger, J. 2010. Managing risks in the supply chain: Useful tips. *Compliance Week* (May): 54–56.

Jensen, M., and W. Meckling. 1976. Theory of the firm: Managerial behavior, agency costs, and capital structure. *Journal of Financial Economics* 3: 305–360.

Jorgensen, J. 1996. Managing the risks of outsourced IT. *The Internal Auditor* 53 (6): 54–59.

Kershaw, D. 2005. Evading Enron: Taking principles too seriously in accounting regulation. *Modern Law Review* 68 (4): 594–625.

Klein, R., and A. Rai. 2009. Interfirm strategic information flows in logistics supply chain relationships. *MIS Quarterly* 33 (4): 735–762.

Kobelsky, K., V. J. Richardson, R. E. Smith, and R. W. Zmud. 2008a. Determinants and consequences of firm information technology budgets. *The Accounting Review* 83 (4): 957–995.

Kobelsky, K., S. Hunter, and V. J. Richardson. 2008b. Information technology, contextual factors and the volatility of firm performance. *International Journal of Accounting Information Systems* 9 (3): 154–174.

Lee, S., K. Lee, and W. Kang. 2005. Efficiency analysis of controls in EDI applications. *Information & Management* 42 (3): 425–439.

Lewin, A. Y., and C. Peeters. 2006. Offshoring work: Business hype or the onset of fundamental transformation? *Long Range Planning* 39 (3): 221–239.

Li, C., G. F. Peters, V. J. Richardson, and M. W. Watson. 2012. The consequences of information technology control weaknesses on management information systems: The case of Sarbanes-Oxley internal control reports. *MIS Quarterly* 36 (1): 179–203.

Libby, R., and N. Seybert. 2009. Behavioural studies of the effects of regulation on earnings management and accounting choice. In *Accounting, Organizations, and Institutions: Essays for Anthony Hopwood*, edited by Chapman, C. Cooper, D. and Miller, P. Oxford, U.K.: Oxford University Press.

Lund-Thomsen, P. 2008. The global sourcing and codes of conduct debate: Five myths and five recommendations. *Development & Change* 39 (6): 1005–1018.

Manning, S., A. Y. Lewin, and M. Schuerch. 2011. The stability of offshore outsourcing relationships: The role of relation specificity and client control. *Management International Review* 51: 381–406.

McCray, S. 2008. *The Top 10 Problems with Outsourcing Implementations (and How to Overcome Them)*. Technology Partners International, Inc. Available at: http://www.tpi.net/pdf/papers/Top_10_Problems-with_Outsourcing.pdf

McFarland, R. G., J. M. Bloodgood, and J. M. Payan. 2008. Supply chain contagion. *Journal of Marketing* 72 (2): 63–79.

Merchant, K. A., and W. A. Van der Stede. 2007. *Management Control Systems: Performance Measurement, Evaluation, and Incentives*. 2nd edition. Upper Saddle River, NJ: Prentice Hall.

Miller, S. K. 2009. *Choosing an Outsourced Service Provider: Consider Accountability & Quality of Service before Turning over Your Operations*. Available at: http://www.processor.com/editorial/article.asp?article=articles%2Fp3113%2F10bp13%2F10bp13.asp

Morris, J. J. 2011. The impact of enterprise resource planning (ERP) systems on the effectiveness of internal controls over financial reporting. *Journal of Information Systems* 25 (1): 129–157.

Murthy, U., and J. L. Reck. 2012. *The Relationship Between Information Technology Innovation and Material Weaknesses in Internal Control*. Working paper, University of South Florida.

Ngwenyama, O., and N. Bryson. 1999. Making the information systems outsourcing decision: A transaction cost approach to analyzing decision problems. *European Journal of Operational Research* 115: 351–367.

Nicolaou, A. I., K. L. Sedatole, and N. K. Lankton. 2011. Integrated information systems and alliance partner trust. *Contemporary Accounting Research 28* (3): 1018–1045.

Oh, W., J. W. Kim, and V. J. Richardson. 2006. The moderating effect of context on the market reaction to IT investments. *Journal of Information Systems* 20 (1): 19–44.

Ojo, M. 2010. *International Framework for Liquidity Risk Measurement, Standards and Monitoring, Corporate Governance and Internal Controls*. Available at: http://ssrn.com/abstract=1584402

Ojo, M. 2011. Building on the trust of management: Overcoming the paradoxes of principles-based regulation. *Banking & Financial Services Policy Report* 30 (7): 1–9.

Piccoli, G., and B. Ives. 2005. IT-dependent strategic initiatives and sustained competitive advantage: A review and synthesis of the literature. *MIS Quarterly* 29 (4): 747–776.

Premkumar, P., V. J. Richardson, and R. W. Zmud. 2004. Sustaining competitive advantage through a value net: The case of Enterprise Rent-A-Car. *MIS Quarterly Executive* 3 (December): 189–199.

Public Company Accounting Oversight Board (PCAOB). 2007a. *An Audit of Internal Control over Financial Reporting that Is Integrated with an Audit of Financial Statements*. Auditing Standard No. 5. Washington, DC: PCAOB.

Public Company Accounting Oversight Board (PCAOB). 2007b. *Report on the PCAOB's 2004, 2005, and 2006 Inspections of Domestic Triennially Inspected Firms*. Washington, DC: PCAOB.

Ren, K., C. Wang, and Q. Wang. 2012. Security challenges for the public cloud. *IEEE Internet Computing* 16 (1): 69–73.

Schwarcz, S. L. 2009. The "principles" paradox. *European Business Organization Law Review* 10: 175–184.

Simons, R. 1995. *Levers of Control: How Managers Use Innovative Control Systems to Drive Strategic Renewal*. Boston, MA: Harvard Business School Press.

Stefaniak, C. M., R. W. Houston, and R. M. Cornell. 2012. The effects of employer and client identification on internal and external auditors' evaluations of internal control deficiencies. *Auditing: A Journal of Practice & Theory* 31 (1): 39–56.

Sullivan, W. E., and O. Ngwenyama. 2005. How are public sector organizations managing IS outsourcing risks? An analysis of outsourcing guidelines from three jurisdictions. *Journal of Computer Information Systems* 43 (3): 73–87.

Tuttle, B., and S. Vandervelde. 2007. An empirical examination of COBIT as an internal control framework for information technology. *International Journal of Accounting Information Systems* 8: 240–263.

U.S. House of Representatives. 2002. The Sarbanes-Oxley Act of 2002. Public Law 107-204 [H.R. 3763]. Washington, DC: Government Printing Office.

Vasarhelyi, M. A., M. Alles, and A. Kogan. 2004. Principles of analytic monitoring for continuous assurance. *Journal of Emerging Technologies in Accounting* 1 (1): 1–21.

Vathanophas, V. 2007. Business process approach towards an inter-organizational enterprise system. *Business Process Management Journal* 13 (3): 433–450.

Wallace, L., H. Lin, and M. A. Cefaratti. 2011. Information security and Sarbanes-Oxley compliance: An exploratory study. *Journal of Information Systems* 25 (1): 185–211.

Wolfe, C. J., E. G. Mauldin, and M. C. Diaz. 2009. Concede or deny: Do management persuasion tactics affect auditor evaluation of internal control deviations? *The Accounting Review* 84 (6): 2013–2037.