How to Manage Section 404 of The Sarbanes-Oxley Act: What Is Wrong with Section 404 of the Sarbanes-Oxley Act?

Heng-Hsieu Lin
University of Portland

Frederick H. Wu
University of North Texas

Abstract

The paper begins with explaining the concept of internal control according to COSO’s (Committee of the Sponsoring Organizations of the Treadway Commission) 1992 pronouncement. Next, the main section of the paper explains how all significant enterprise-wide risks, not just the risks existing in accounting systems, affect financial reporting. The presentation in this section of control over the management process is not found anywhere in the internal control literature and official pronouncements. The paper ends with a recommendation that every business organization adopt COSO’s new pronouncement, Enterprise Risk Management—Integrated Framework, to establish and implement an effective enterprise-wide system of internal control, based on risk analysis.

Keywords: Sarbanes-Oxley Act · Internal Control
如何操弄沙賓法案 404 節：沙賓法案 404 節有何問題？

Heng-Hsieu Lin
University of Portland

Frederick H. Wu
University of North Texas

摘要

本文首先依 COSO 1992 年公報解釋內部控制之觀念，其次說明所有重大之全面性企業風險如何影響財務報導，並非只有會計系統所存在之風險才會影響財務報導。本文所描述管理過程之控制並未見之於其他內部控制文獻或正式公報。最後，本文建議企業採用 COSO 新公報時應基於風險分析，建立及執行有效的全面企業內部控制制度。

關鍵詞：沙賓法案、內部控制
Section 404 of the Sarbanes-Oxley Act of 2002 (hereafter referred to as Section 404) requires management and independent auditors to report on the effectiveness of internal control over financial reporting. What is new in Section 404 is the mandatory reports on internal control by management and independent auditors, but not the concept of internal control. Its main thrust is that, if management and independent auditors are required to provide such reports, corporate scandals such as Enron and WorldCom could be prevented. The thrust is misconstrued since, first of all, the concept of internal control is nothing new and never designed to be a panacea for corporate ills. Traditionally in the audit literature, the concept of internal control is narrow in scope and procedural in application. It is narrow because the scope of internal control is largely confined to accounting systems to support the accounting process. It is procedural because auditors tend to follow a set of prescribed mechanical procedures to determine whether or not internal control surrounding and embedded in accounting systems is reliable. Auditors, in general, will not concern themselves with controls beyond the accounting process. This is where the problem of the traditional internal control concept lies.

Secondly, the Foreign Corrupt Practices Act of 1976 (enacted by Congress) has already defined the responsibilities of corporate management regarding the establishment of an effective system of internal control. Accordingly, the mechanism of corporate governance through internal control has been legally declared mandatory since then. Section 404, in essence, renews the enforcement of the Foreign Corrupt Practices Act. However, the failure of the Act should have conveyed potential difficulties in the implementation of Section 404.

Thirdly, as far as requiring independent auditors to attest to and render an opinion on, the effectiveness of internal control, that is nothing new either. The evaluation of internal control is an integral part of a financial audit. The scope of the audit is based on the assessment of the strengths and weaknesses of the internal control for the client’s accounting systems. At the end of an audit engagement, independent auditors generally provide a management report that will include recommendations to strengthen internal control if it is found to be significantly weak. If management uses the auditor’s report to improve internal control, with the auditor required by Section 404 to attest to management’s assertions about the effectiveness of internal control, there would arise the age-old issue of the conflict of interest.

Section 404 addresses symptoms more than causes. Why? The answer to this question is the purpose of this paper. The paper begins with explaining the concept of internal control according to COSO’s (Committee of the Sponsoring Organizations of the Treadway Commission) 1992 pronouncement. (Note that the AICPA’s Statement on
Auditing Standards No. 55 and No. 78 adopt COSO’s recommendations). Next, the main section of the paper explains how all significant enterprise-wide risks, not just the risks existing in accounting systems, affect financial reporting. The presentation in this section of control over the management process is not found anywhere in the internal control literature and official pronouncements. The paper ends with a recommendation that every business organization adopt COSO’s new pronouncement, *Enterprise Risk Management—Integrated Framework*, to establish and implement an effective enterprise-wide system of internal control, based on risk analysis.

1. CORPORATE SCANDALS NOT ACCOUNTING SCANDALS

Accounting did not cause the recent corporate scandals such as Enron and WorldCom. Unreliable financial statements were the results of management decisions, fraudulent or not. To blame fraudulent financial statements for management’s misdeeds is only an attempt to cast accountants as the scapegoats and misses the real issue of corporate scandals. It is true that reliable financial reports rely, to a certain extent, on effective internal controls, but it is also true that effective internal controls rely, to a large extent, on a reliable management system coupled with strong corporate governance. (A management system is a process of planning, executing and control for all business processes in an organization.) Management systems dictate all business processes. When management deliberately or even unlawfully manipulated business processes in order to achieve desirable financial goals and presented untruthful financial reports to the public, accounting systems were abused and became a victim rather than a perpetrator of such scandals. Internal control, no matter how effective, is rendered impotent when and if management decides to circumvent it. Therefore, internal control must be extended to cover all major risks outside of the accounting process. In other words, internal control rests on adequate and comprehensive analysis of enterprise-wide risks.

2. DEFINITION AND PURPOSES OF INTERNAL CONTROL

According to COSO, internal controls encompass a set of policies, rules and procedures enacted by the management of the firm to provide reasonable assurance that (1) financial reporting is reliable, (2) its operations are effective and efficient, and (3) its activities comply with applicable laws and regulations\(^1\). This definition clearly indicates that internal control has multiple purposes, not just reliable financial reporting. In fact, it implies that internal control deals with potential risks existing in three areas of business:

information processes (capturing data, maintaining databases, and providing information to achieve reliable financial reporting), operation processes (activities in the value chain to achieve operational efficiency and effectiveness), and compliance processes (the objective of conformity with laws and regulations). The most crucial process of all in every organization, however, is the management process, referred to as the management system above, that dictates and controls all other business processes. (In this paper, the term “business processes” refers to the combination of the management, operation, information and compliance processes.) Lack of attention to internal controls in the management process is another major weak spot of the traditional internal control concept. Risks in the management processes are much more critical, an issue we will explore further later. It is important to note that significant potential risky events in every business process, if actually occurred, can contribute to failures of internal control over financial reporting. Risks in the information process are not the only source of failure of internal control over financial reporting. Thus, a better way to state the requirement of Section 404 is:

Management and independent auditors are required to report on the effectiveness of internal control over enterprise risks affecting financial reporting.

An effective system of internal control must be built on the basis of the analysis of enterprise-wide risks.

Traditionally, independent auditors focus on risks directly related to business transactions defined by generally accepted accounting principles and therefore, risks in the information process are the focal points in the evaluation of the strengths and weaknesses of internal control. Risks, however, exist in every business process and some of those risks, if and when materialized, will affect financial reporting significantly. As a matter of fact, major enterprise risks rarely occur within the accounting process. How may cases were there in which business organizations were toppled by the failures of information systems? Recent corporate malfeasances such as Enron and WorldCom were the results of risks realized in the management process and other major business processes.

No wonder, COSO, first, proposed that risk analysis be one of the five components making up the system of internal control in its 1992 pronouncement. Then in September 2004, it extended and refined the original concept of risk analysis by proposing an integrated framework for enterprise risk management. “Enterprise risk management is a process, effected by an entity’s board of directors, management and other personnel, applied in strategy settings and across the enterprise.”² It is designed to manage risk for

---

providing reasonable assurance regarding the achievement of the following entity objectives:

- Strategic – high-level goals, aligned with and supporting its mission
- Operations – effective and efficient use of its resources
- Reporting – reliability of financial reporting
- Compliance – compliance with applicable laws and regulations.

Thus, in the process of creating value for its customers and stockholders, an entity must be able to systematically assess and analyze all material risks affecting the aforementioned entity objectives.

### 3. STRATEGIC AND DECISION RISKS

Every entity, whether for-profit or not-for-profit, exists to create value for its stakeholders. In the course of creation of value, the entity’s management has to follow a process to make important decisions regarding goals, strategies, and resource acquisition and allocation for all of its operations—this is the planning stage of the so-called management system or process. After a strategic plan is formulated, the process moves to the stages of execution (of the plan) and control (of operations). The process ends with an assessment of the results of operations relative to the strategic plan by means of the entity’s information systems, mainly accounting systems. Information as the result of measurement serves management for making further decisions regarding goals, strategies, and resources allocation. Thus, the strategic planning cycle starts all over again.

All the decisions made in the management process entail uncertainties—unattainable goals due to fatal strategies, and operational failures due to inefficient allocation and ineffective application of resources. The chosen strategy presents risks associated with competition in the market place. The allocation and application of resources presents risks associated with quality and marketability of products or services to customers. Decisions about strategic and resource choices are the most critical issues to every business entity, because most business failures are due to strategic errors or inefficient and ineffective operations leading to the production of uncompetitive products or services.

It then becomes obvious that internal controls must function effectively in the management process. Policies and procedures must be established to govern the strategic planning process. In particular, accounting systems must have the mechanism of measuring strategic variables to highlight strategic success or failure. Information
about strategic success or failure must be provided to the board of directors for effective monitoring. The tricky part of assessing strategic results is how to unravel legally questionable management decisions that are hidden behind financial numbers presented in the quarterly and annual financial reports. Currently, internal controls for the management process in many business entities are either lacking or working poorly, and this explains why there were so many corporate scandals in the past decade. Enron’s strategy to create special purpose entities was a strategic risk as well as a decision risk.

Bristol-Myers “channel stuffing” (loading wholesalers with merchandise at the end of a period) is an operational risk (to be discussed later) as well as a decision risk. Arthur Andersen’s shredding documents related to Enron’s audit is a strategic risk as well as a decision risk.

4. INFORMATION PROCESS AND RISKS

Information process refers to the sequential events of capturing business transaction data, maintaining databases or master files, and providing information from databases to internal users for managerial planning and control and external users for making financing and investment decisions. The process, if supported by accounting systems, is also called the accounting process. Data capturing is the most crucial event in the accounting process because most cases of unreliable financial reporting are the results of data manipulation, and also because internal controls are generally designed to capture more unintentional data errors than intentional ones. Capturing erroneous data will lead to generating unreliable financial reports regardless of how good accounting systems are. Remember the well-known expression, “garbage in garbage out”. Erroneous data, intentional or unintentional, poses information risks in financial reporting if errors are significant or material. To prevent data errors and minimize input risks, control devices (policies, rules, procedures and methods), generally referred to as “input controls”, are established. Policies, rules, and procedures are described in the accounting and various other operational policy and procedure manuals in every business entity. Methods or techniques are tools to implement control policies, rules, and procedures, such as passwords, firewalls, and back-up systems.

No matter how many input controls an entity has designed and established, internal control may not be able to handle uncertainties related to the performance estimates of an entity’s certain financial variables—estimates that must be made for financial reporting. To cite a few examples: banks’ bad debt reserves, property and casualty insurers’ loss reserves, and corporations’ assumed earnings rate on pension assets. What can internal control do with regard to the reliability of these estimates? The risks
with these estimates of reserves are high and real. What can internal control do with Clear Channel’s recent $4.9 billion write-off and the recent restatements by restaurant companies for lease accounting and GE’s recent restatement for derivatives?

The key point is that accounting data is not all factual and empirically verifiable. Some of the financial estimates mentioned above are probabilistic (e.g., bad debts and casualty loss reserves); some are logical (e.g., depreciation and amortization); and some are subjective (e.g., bank cash reserves or goodwill). How can an auditor apply internal control to the audit of net income that is determined from aggregations of factual data, probabilistic data, logical data and subjective data? How can an auditor say that financial statements are reliable when a probabilistic data represents the probable results of a future event, logical data may be illogical when circumstances have changed, and subjective data are simply subjective. That is why internal control is not a panacea for solving corporate scandals.

Errors can occur and lead to information risks during the processing of data to maintain databases or master files. Thus, internal controls are also designed to prevent and detect errors and to minimize risks at this stage of the information process. This area of controls is generally referred to as “processing controls” in the internal control literature. Various systems documentation manuals in business entities prescribe how systems should be operated in order to process transactions accurately. These manuals are established policies, rules, and procedures that system operation personnel must follow in order to maintain reliable databases or master files from which financial information is to be produced. These manuals give rise to the design of tools that can provide reasonable assurance that data are correctly processed. Examples of such tools are test data, edit programs, run-to-run reconciliation, etc.

Finally, errors can occur and risks can become real due to lack of controls over the access to financial information. A particular concern of any business entity in this area of the information process is the protection of sensitive information. Internal controls, generally referred to as output controls, are designed to handle the potential risks of losing or abusing sensitive financial data. Again, similar to controls for input and processing, policies, rules, and procedures should be established to control errors and minimize risks in handling information, the output of the accounting systems.

Effective input-processing-output controls, generally referred to as application controls, are not sufficient to ensure reliable financial reporting if there is a poor control environment surrounding the applications of information technologies (IT). For example, if a firm does not build a culture of ethical behavior for its employees over years, all controls the firm has established over input, processing, and output in the information process could be either circumvented or tempered. As another example, if
management has decided to smooth earnings by inflating sales at year-end, the deliberate misrepresentation of sales in the financial reports would actually mock internal control in accounting systems. Internal controls to handle risks outside of accounting systems are generally referred to as general controls, encompassing proper separation of duties in accounting department and between users departments and IT department, physical assess and security, logical access controls, systems development standards, contingency or recovery plans, etc. COSO treats this area of control as the control environment of the entity, but subsequently renames it as the internal environment, one of the components of the enterprise risks management.

5. OPERATION PROCESSES AND RISKS

General and application controls cannot be adequate unless risks in the operation processes are also effectively monitored. Operational processes are the primary and supportive activities in the value chain. Primary activities, namely acquisition of resources, conversion of resources to products or services, and distribution, marketing and sales of products and services, create products or services which customers are willing to pay for. Business entities create value through these primary activities. Supportive activities such as research and development, management, information technology, and organizational structure are designed to enhance the operational efficiency and effectiveness of primary activities.

The risks of producing unreliable financial reports could exist in any operation process. For example, improper handling of sales and purchase procedures could lead to overstatement of sales and understatement of costs in the financial statements--which is an operational risk, if not detected and prevented. As another example, if the sales management of a telecommunication company treats intra- or inter-company transactions as sales, when, in fact, they are merely asset transfers, the intentional misrepresentation of the bogus sales in the financial reports is the result of the covert operation in the sales process, having nothing to do with internal controls in the accounting systems. So, information risks pose as threats simply due to control deficiencies in the operation processes.

Efficiency and effectiveness of the operation processes is one of the three control objectives of internal control as defined by COSO and pointed out earlier. Failure in this objective could lead to failure in financial reporting. Some of the recent sensational corporate news were the results of control failures in the operation processes. These include Tyco’s handling of employee loans, Enron’s handling of financial obligations to subsidiary (special purpose) companies, and AIG’s (American International Group)
handling of risk-free insurance. In these cases, accounting systems captured data from ill-conceived transactions that occurred in the business processes and were conveyed to the accounting system as authorized and genuine transactions. When erroneous transactions are treated as if they were authenticated in the operation processes, controls break down and the realized operation risks give rise to financial reporting failures.

If business history tells us that financial reporting failures were due to control deficiencies in the operation processes, operation management must be made responsible for the establishment of an effective system of internal control. Currently, the blame for such failures, placed on the accounting system, is to misplace the causes underlying the failures. Internal control should permeate every segment of the entity’s business and should be the concern of all operation management, not just management in the accounting process. This is the spirit of what COSO defines as the control environment of the business entity.

6. COMPLIANCE RISKS

For financial reporting, every public company must comply with applicable laws and regulations of the Securities and Exchange Commission (SEC) and the Public Company Accounting Oversight Board (PCAOB). The SEC and the PCAOB were both created by Congress to regulate accounting practices of public companies. Violations of laws and regulations under their oversight may be deemed criminal.

Criminal violation of specific federal laws and regulations in specific industries may also occur. For example, the Federal Banking Administration has specified banking laws and regulations for banks to follow. Similar situations exist in various industries such as insurance, investment, and airlines. In addition, at the state level, every business entity must also comply with state laws and regulations applicable to the entity’s business.

Violation of federal and state laws and regulation can jeopardize an entity’s financial condition and its survival, as exemplified by the demise of several public companies in the past decade. Thus, control policies, rules, and procedures must be established to reduce the risks of noncompliance. The responsibility of enforcing compliance policies, rules, and procedures rests with the operation units whose operations are affected by applicable laws and regulations. The risks of noncompliance, thus, exist in the operation processes and they, if actually occurred, can significantly affect an entity’s operational results and financial condition.
7. A FRAMEWORK OF ENTERPRISE RISK MANAGEMENT AND INTERNAL CONTROL

As stressed earlier, an effective system of internal control in a business entity must build on the foundation of effective management of enterprise risks: strategic and decision risks, information systems risks, operation risks, and compliance risks. This is what COSO advocates in its new publication, Enterprise Risk Management – Integrated Framework. Enterprise risk management is defined as follows:

“Enterprise risk management is a process, effected by an entity’s board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.”

The objectives to be achieved by enterprise risk management are: strategic goals, operational effectiveness and efficiency, reliable financial reporting, and compliance with applicable laws and regulations. Except for strategic goals, the other three objectives are defined under the objectives of internal control previously defined by COSO in its 1992 pronouncement.

The four objectives of enterprise risk management can be accomplished by managing the four types of risk stated above. Strategic and decision risk analysis will lead to establishing required internal controls to achieve the strategic goals, that is, creating value for stakeholders. Information risk analysis will lead to developing internal controls to accomplish the goal of reliable financial reporting. Operation risk analysis will help establish internal control needed to accomplish the goal of operational effectiveness and efficiency. Finally, compliance risk analysis will help identify required internal controls for achieving the compliance goal.

Figure 1 presents a diagram that describes the relationship between risk analysis and internal control. It starts with a classification of employees into operation, compliance, information, and management. First, operation employees are to execute events in the operation processes in accordance with the policies, rules and procedures (control procedures) established to govern the processes, but they may execute improperly, giving rise to operation risks. The risks, if significant or material, will have an impact on the information process, leading to information risks. Second, managers in executing events related to strategic and other decisions in the management process may entail strategic risks and/or decision-making risks, both of which, if realized, may likely contribute to information risks. Internal controls must be established for mitigating

---

these two types of risks in the management process. Strengthening corporate governance, for example, through an independent board of directors and audit committee is recommended by the Sarbanes-Oxley Act to counteract the management process risks. Third, controls are established to combat threats from events related to noncompliance with applicable laws and regulations.

All the events that may pose as risks in various business processes are filtered through respective systems of internal control, and, if these risks are material and not detected and prevented, will be filtered one more time through controls in the accounting information process. As presented in Figure 1, all transactions (events) in various business processes may carry with them transaction risks (errors) that are to enter the accounting information process. At this critical stage, operation risks, management risks, and compliance risks may all become a part of information risks. To overcome these risks, general and application controls are designed, tested, and implemented. The preventive type of controls is particularly important to ensure that only correct data is entered in accounting systems. However, the established preventive input controls, no matter how effective they are, cannot not detect all material risks from the operation and compliance processes. Furthermore, managers may decide to circumvent the system of internal control in the accounting process and render internal control futile. The decisions made in the management process can overrule all controls in the accounting process.

When risks from operation and management processes as well as risks within the information process become realized, accounting systems will be contaminated with errors and mistakes in data. In addition, risks within the information process emerge when non-factual data (estimates) are created for bad debts, pension funds return rates, goodwill, depreciation and amortization, etc. These errors, if significant or material and if not detected and corrected, will lead to creation of financial statements which are not fairly presented.

The above explanation of the concepts of internal control and enterprise risk management (ERM) is recapped in Figure 2. Before trying to understand Figure 2, we must first understand that “internal control is encompassed within an integral part of ERM. ERM is broader than internal control, expanding and elaborating on internal control to form a more robust conceptualization, focusing more fully on risk.”3 (COSO, 2004, p. 109). Figure 2 captures the spirit and substance of COSO’s ERM that is intended to provide reasonable assurance for accomplishing every business entity’s four objectives: strategic, operation, reporting, and compliance. The realization of these four objectives is, as the entity’s mission, to create value for stakeholders.

ERM is composed of eight (8) components: internal environment, strategic...
objectives, event identification, risk assessment, risk response, control activities, information and communication, and monitoring. This is certainly an extension of the five components of internal control, which are control environment, risk analysis, control activities, information and communication, and monitoring. The extension stresses the critical aspect of risk analysis in the process of implementing internal control. In other words, internal control will not be complete and adequate without doing risk analysis first.

Similar to the concept of control environment defined as the first component of internal control by COSO, the Internal Environment sets the tone of an organization, influencing the risk consciousness of its people, and is the basis for all other components of ERP. After an analysis of internal environment is completed, an organization is set to define its Objectives at the strategic level, establishing a basis for operations, reporting, and compliance objectives. With objectives established, the organization should proceed to Identify Events that affect the achievement of objectives favorably and unfavorably. Favorable events represent opportunities for the organization and should be pursued by its management regarding resource allocation decisions to capitalize those opportunities.

Unfavorable events represent risks that must be analyzed in order to determine the extent of its financial compact and how the business entity is going to respond to them—this constitutes the two essential components of ERM: Risk Assessment and Risk Response. Once significant risks are identified and analyzed and the risk response policies are established, internal control is logically and subsequently designed and implemented to prevent them from occurrence. This is what COSO refers to as control activities of ERM. Internal control in the context of today’s technological environment encompasses general control and application controls as expounded earlier.

Effective implementation of ERM relies on accounting information systems to capture data regarding results of execution of strategic, operational and compliance activities relative to the pre-set goals and to communicate information about these results to various levels of management for refining the ERM process. The results should also be communicated to employees of the entity so that ERM becomes, not just managers’, but also everyone’s business. This is the Information and Communication component of ERM. Finally, as ERM is defined as a process, it must be Monitored (the last component) to be effective.
8. CONCLUSION

The above delineation of internal control and ERM may be summarized as follows:

• ERM is an effective way to handle Section 404. According to COSO, ERM is more than just internal control. Its ultimate goal is the creation of value for stakeholders.

• Risk analysis provides a basis for the design and implementation of an effective system of internal control for an entire business entity.

• Risk analysis must be conducted in all business processes: management, operation, information, and compliance.

• The most critical of all business processes is the management process that focuses on strategies and objectives and may entail strategic and decision risks. Internal control must be established to counteract this area of business risks, otherwise financial reports will likely be manipulated, giving rise to more cases similar to Enron and WorldCom.

• Risks in the operation process and the compliance process, if not detected and prevented, may also contribute to information risks. Separate internal controls are needed to control operation and compliance activities.

• Risks in the information process lies primarily with those estimates for some financial variables that are subject to manipulation.

• Internal control is no panacea for detecting major business problems. An effective system of internal control can provide only reasonable assurance that an entity’s strategic and other ensuing objectives will be achieved.
Figure 1: A System of Internal Control based on Risk Analysis for Reliable Financial Reporting

Operation Employees → Compliance/Information Personnel → Management

Events → Operation Process Risks → Compliance Process Risks → Management Process Risks

Filtering → Internal controls → Internal controls → Internal controls

Transaction Data → Accounting Systems → Transaction Data

Information Process Risks

Filter

Internal Controls: General Controls and Application Controls

Reliable Financial Statements

Figure 2: An Enterprise Risk Management Framework for Creating Value to Stakeholders

A Process (System)

Internal environment
Objective Setting: Mission, goals and strategies for value creation
Event Identification
Risk Assessment → Strategic and decision risks
→ Operation risks
→ Information risks
→ Compliance risks
Risk Response
Control Activities: A system of the enterprise-wide internal control
Information and communication
Monitoring

To provide Reasonable assurance regarding:

Strategic alliance with mission and goals
Reliable financial reporting
Operational efficiency and Effectiveness
Compliance with applicable laws and regulations