Limitations of Section 404 of the Sarbanes-Oxley Act

By Heng Hsieu Lin and Frederick H. Wu

Section 404 of the Sarbanes-Oxley Act of 2002 (SOX) requires management and independent auditors to report on the effectiveness of internal control over financial reporting. The concept of internal control is not new; what section 404 introduces is mandatory reports on internal control by management and independent auditors. The belief behind the requirement is that such audited reports could prevent corporate scandals such as Enron and WorldCom.

This aim is misguided for a number of reasons. First, internal control was not conceptually 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 internal controls surrounding and embedded in accounting systems are reliable. In general, auditors will not concern themselves with controls beyond the accounting process. This is where the problem of the traditional internal control concept lies.

Second, the Foreign Corrupt Practices Act of 1976 (FCPA) defines 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 mandatory since then. Section 404, in essence, renews the enforcement of the Foreign Corrupt Practices Act. However, the failure of the FCPA should have conveyed the potential difficulties in the implementation of SOX section 404.

Third, requiring independent auditors to attest to and render an opinion on the effectiveness of internal control is nothing new. 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 internal control over a company's accounting systems. At the end of an audit engagement, independent auditors generally provide a management report that includes 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, conflict-of-interest issues would be raised.

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 otherwise. To blame management's misdeeds on fraudulent financial statements casts accountants as the scapegoats and misses the real issue. Reliable financial reports rely to a certain extent on effective internal controls, but 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 manipulates business processes in order to achieve desirable financial goals and present untruthful financial reports to the public, accounting systems are abused and victims rather than perpetrators. Internal control, no matter how effective, is rendered impotent when 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.

Definition and Purposes of Internal Control

According to the *Internal Control–Integrated Framework*, issued by the Committee of Sponsoring Organizations (COSO) in 1992, internal controls encompass a set of policies, rules, and procedures enacted by management 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. This definition clearly indicates that internal control has purposes other than 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 is the management process, referred to above as the management system, that dictates and controls all other business processes. ("Business processes" as used in this article 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; it has not been explored and stressed in the internal control literature. Risks in the management processes, dis-

cussed below, are much more critical. Significant potential risky events in every business process, if they do occur, 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 (GAAP), 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 risks, if and when their related events materialize, will significantly affect financial reporting. In fact, major enterprise risks rarely occur within the accounting process. Recent corporate malfeasances such as Enron and WorldCom were the results of risks realized in the management process and other major business processes, and are examples of businesses that have been toppled by the failures of information systems.

It is not surprising that COSO proposed risk analysis as one of the five components of internal control in its 1992 pronouncement. In September 2004, COSO extended and refined the original concept of risk analysis by proposing an integrated framework for enterprise risk management, which is designed to manage risk by 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; and
- Compliance: compliance with applicable laws and regulations.

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

Strategic and Decision Risks in the Management Process

Every entity, whether for-profit or not-for-profit, exists to create value for its stakeholders. In the course of creating 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 the entity formulates a strategic plan, 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 as compared to the strategic plan by means of the entity's information systems, mainly accounting systems. This information serves management in making further decisions regarding goals, strategies, and resource allocation, and the strategic planning cycle begins again.

All 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 marketplace as well as with hard-to-predict economic, political, and social events. Allocating and applying resources presents risks associated with the quality and marketability of products or services. 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 that lead to uncompetitive products or services.

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 difficult part of assessing strategic results is unraveling legally questionable management decisions that are hidden in the quarterly and annual financial reports. Currently, internal controls for the management process in many business entities are either lacking or working poorly. Enron's strategy to create special purpose entities was a strategic risk as well as a decision risk. Arthur Andersen's shredding of documents related to Enron's audit was a strategic risk as well as a decision risk.

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 to external users for making financing and investment decisions. This 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. As the saying goes, Garbage in, garbage out. No matter how good the accounting systems are, erroneous data lead to unreliable financial reports. If errors are significant or material, erroneous data, intentional or unintentional, pose information risks in financial reporting. To prevent data errors and minimize input risks, control devices (policies, rules, procedures, and methods), generally referred to as "input controls," are established. Input controls are particularly necessary in order to prevent accounting managers, in cooperation with the CEO, from initiating fictitious transactions.

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 certain financial variables that must be made for financial reporting. Examples include banks' bad-debt reserves; property and casualty insurers' loss reserves; and corporations' assumed earnings rate on pension assets. The risks with these estimates of reserves are high and real. Real-world examples include Clear Channel's $4.9 billion write-off, restatements by restaurant companies for lease accounting, and GE's restatement for derivatives.

The key point is that not all accounting data are factual and empirically verifiable. Some of the aforementioned financial estimates 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). An auditor cannot simply say that financial statements are reliable when probabilistic data represent the probable results of a future event, that logical data may be illogical when circumstances have changed, or that subjective data are simply subjective. That is why internal control is not a panacea.

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

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 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, policies, rules, and procedures should be established to control errors and to minimize risks in handling the accounting system's information output.

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 time, controls in the information process could be circumvented or tempered.

Internal controls to handle risks outside of accounting systems are generally referred to as general controls, encompassing proper separation of duties in the accounting department and between users' departments and the IT department, physical assess and security, logical access controls, systems development standards, and contingency or recovery plans. COSO treats this area as the control environment of the entity, but subsequently renames it as the internal environment, one component of enterprise risk management.

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 that customers are willing to pay for. Business entities create value through these primary activities. Supportive activities, such as research and development, management, IT, 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—an operational risk, if not detected and prevented. Or, if the sales management of a telecommunication company treats intra- or intercompany transactions as sales, 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 threats simply due to control deficiencies in the operation processes.

As stated previously, efficiency and effectiveness of the operation processes is one of three control objectives of internal control as defined by COSO. Failure in this objective could lead to failure in financial reporting. Recent sensational corporate news stories that were the result of control failures in operation processes include controversies over Tyco's handling of employee loans and AIG's handling of risk-free insurance. In these cases, accounting systems might have 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, leading to financial reporting failures.

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

Compliance Risks

For financial reporting, every public company must comply with applicable laws and regulations issued by the SEC and the Public Company Accounting Oversight Board (PCAOB). Violations of laws and regulations under their oversight may be deemed criminal. For example, banks have specific laws and regulations to follow. Similar situations exist in other industries. 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 regulations 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. Responsibility for enforcing compliance policies, rules, and procedures rests with the units whose operations are affected by applicable laws and regulations. Therefore, the risks of noncompliance exist in the operation processes and, if related events actually occur, they can significantly affect an entity's operational results and financial condition.

A Framework for Enterprise Risk Management and Internal Control

Of the aforementioned types of risks, the PCAOB appears to focus on information risks. In Auditing Standard 2 (2004), the

DELINEATION OF INTERNAL CONTROL AND ENTERPRISE RISK MANAGEMENT

- Enterprise Risk Management (ERM) is an effective way to handle SOX section 404. According to COSO, ERM is more than 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 business process is the management process that focuses on strategies and objectives. It may entail strategic and decision risks. Internal control must be established to counteract this area of business risk; otherwise, financial reports will likely be manipulated. (This area of internal control has not been addressed by either COSO or the PCAOB.)
- 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. (This area of internal control has not been emphasized by the accounting profession.)
- Risks in the information process lie 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.

PCAOB defines internal control as follows:

> A process designed by, or under the supervision of, the company's principal executives ... to provide reasonable assurance regarding the reliability of financial reporting and preparation of financial statements for external purposes ... [including] those policies and procedures that:
>
> 1) pertain to the maintenance of records that, in reasonable detail, accurately and fairly reflect the transactions and disposition of the assets of the company;
>
> 2) provide reasonable assurance that transactions are recorded as necessary to permit preparation of financial statements ...
>
> 3) provide reasonable assurance regarding prevention or timely detection of unauthorized acquisition, use or disposition of the company's assets ....

This definition indicates that the objective of internal control is the reliability of financial reporting. The standard does not address internal controls needed for countering operational and compliance risks or controls over the crucial management process.

Business risks in the operation, information, and compliance processes generally will not create as much impact as risks in the management process. The operation, information, and compliance processes comprise repetitive and horizontally sequential events that are easily automated. Enterprise resource planning (ERP), electronic data interchange (EDI), supply-chain management (SCM), and customer-relation management (CRM) software renders these business processes efficient and effective. At the same time, IT embedded into these processes also captures and processes business data effectively and efficiently. The same cannot be said for the management process.

Another important point is the pervasive application of IT in business. Information processes are embedded into operation processes, meaning that the two have to work together to achieve the desired level of efficiency and effectiveness. This implies that information risks are interlocked with operation risks. This also means that internal controls for information processes must be designed in conjunction with the design of internal controls for operation risks.

Furthermore, if the operation, information, and compliance processes are routine and repetitive, then monitoring (analyzing, assessing, and documenting) risks and internal controls in these processes should be the responsibility of the company's internal auditors, while monitoring risks and internal controls in the management process should be the responsibility of the external auditors. Independent external auditors can evaluate management's decisions more objectively. This division of responsibilities should significantly reduce the costs of implementing SOX section 404 in the long run.

As stressed earlier, an effective system of internal control 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 more than what the PCAOB requires, and it is consistent with what COSO advocates in its new publication, *Enterprise Risk Management—Integrated Framework*, wherein COSO defines enterprise risk management as follows:

> [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, these objectives are defined under the objectives of internal control previously defined by COSO in its 1992 pronouncement. Missing in COSO's strategic risks analysis is accountability of, and subsequently internal controls over, management's decision-making and action.

The four objectives of enterprise risk management can be accomplished by managing the four aforementioned types of risk. 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.

Events that may pose as risks in various business processes are filtered through the respective systems of internal control (see the *Exhibit*). If these risks are high and not detected and prevented, they will be filtered through controls in the accounting information process. 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 are entered in accounting systems. The established preventive input controls, however, no matter how effective they are, cannot 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 thereby render internal control futile. The decisions made in the management process can overrule all controls in the accounting process.

When risky events 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 nonfactual data (estimates) are created. These errors, if significant or material, and if not detected and corrected, will lead to the creation of financial statements that are not fairly presented. ❑

***Heng Hsieu Lin, PhD, CPA`**, is an adjunct professor in the department of accounting at Washington State University at Vancouver, Vancouver, Wash. **Frederick H. Wu, PhD, CMA,** is a professor in the department of accounting of the University of North Texas, Denton, Texas.*

EXHIBIT
A System of Internal Control Based on Risk Analysis for Reliable Financial Reproting