15

Changing Definitions of Internal Control and Information Systems Integrity

R. R. Moeller
Compliance and Control Systems Associates, Inc.
1045 Ridge Avenue
Evanston, IL, USA
Tel. 847-864-2516
Fax. 847-864-5711
robtm1@concentric.net

Abstract

The COSO model of internal control, developed by United States accounting and auditing professionals in 1993, is becoming a worldwide standard for organization internal controls in business and financial systems. In addition to classic financial controls, the COSO model puts a heavy emphasis on information systems. This paper describes the originis of the COSO internal control model, its emphasis on information systems controls , and how the COSO model differs from previous, more narrowly defined internal control models. The strengths and weaknesses of COSO information systems integrity control model is considered as well as the lack of recognition of this model in the more general information system community.

Key Words

COSO, Controls, Internal Control, SAS No. 78, Audit Requirements, Treadway, Standards

1. INTRODUCTION

The 1990s has seen a redefinition of what has traditionally been called "internal control" in the United States. Historically, auditors and accountants defined internal control in terms paper based accounting procedures such as whether a procedure was adequately documented, if appropriate separations of duties and

Integrity and Internal Control in Information Systems Volume 1
S. Jajodia, W. List, G. McGregor & L. Strous (Eds)

responsibilities existed, and the adequacy of batch and other self-balancing control totals. This approach served organizations for many years, but it has become increasingly inappropriate with the growth of highly integrated information systems. For example, a common definition of a separation of duties internal control was that the person opening incoming mail payments should be different than the person taking the checks and making bank deposits. Automation has changed all of this. Many payments today are remitted through electronic data interchange transactions or, soon, through the Internet. Technology has forced organizations to rethink some of these classic internal control rules or standards.

In the United States, many traditional accountants and auditors have historically ignored some of the technology based changes and continued to look for internal control procedures following the older models. However, new standards for internal controls are evolving. They are best defined in the 1992 report (Committee of Sponsoring Organizations of the Treadway Commission, 1992) which has come to be known as the COSO report. While it covers a wide range of internal control issues, the COSO report presents an internal control model that better recognizes information systems technology control and integrity related issues than in the past. From a United States accounting and internal control standards perspective, this paper discusses some of the historical internal control standards that have been in use, the more recent COSO model of internal control, and the information systems control and integrity issues associated with that COSO model. This paper discusses also how the COSO suggested information systems controls match with other recognized models to information systems integrity. The strengths and weaknesses of COSO information systems integrity controls are considered as well as actions to incorporate this COSO model worldwide.

2. EARLIER INTERNAL CONTROL ISSUES

The concept of control or internal control has been used by auditors to define the process of how management mechanisms work since the very early days of auditing. In the past, auditors recognized the need for understanding and evaluating internal control systems (Brink, 1942) and used those definitions of internal control to launch the internal audit profession. Other interested parties, such as the American Institute of Certified Public Accountants (AICPA) in the United States developed their own definitions of internal control that were similar but not totally consistent.

Both the AICPA and the Canadian Institute of Chartered Accountants' (CICA) developed definitions of internal control because of their roles in expressing independent opinions as to the fairness of their clients' financial statements. For example, in the United States, these definitions have been used as a guide by the Securities and Exchange Commission (SEC) in developing regulations covering the enforcement of the Securities Exchange Act of 1934 and later, the Foreign Corrupt Practices Act of 1977. Although there have been changes over the years, the

AICPA's first codified standards were called the Statement on Auditing Standards (SAS No. 1). This standard covered the practice of financial statement auditing in the USA for many years and used the following definition for internal control:

> Internal control comprises the plan of organization and all of the coordinate methods and measures adopted with a business to safeguard its assets, check the accuracy and reliability of its accounting data, promote operational efficiency, and encourage adherence to prescribed managerial policies.

Through clarifications and further definitions, the original AICPA SAS No. 1 then was expanded to define the internal control plan to include two elements:

Administrative controls that includes, but are not limited to, the plan of organization and the procedures and records that are concerned with the decision processes leading to management's authorization of transactions. Such authorization is a management function directly associated with the responsibility for achieving the objectives of the organization and is the starting point for establishing accounting control of transactions.

Accounting controls consist of both the plan of organization and the procedures and records that are concerned with the safeguarding of assets and the reliability of financial records; they are designed to provide reasonable assurance that:

a) Transactions are executed in accordance with management's general or specific authorization.
b) Transactions are recorded as necessary (1) to permit preparation of financial statements in conformity with generally accepted accounting principles or any other criteria applicable to such statement and (2) to maintain accountability for assets.
c) Access to assets is permitted only in accordance with management's authorization.
d) The recorded accountability for assets is compared with the existing assets at reasonable intervals and appropriate action is taken with respect to any differences.

The overlapping relationship of administrative and accounting controls was then further clarified in pre-1988 AICPA standards to state that the foregoing definitions are not necessarily mutually exclusive because some of the procedures and records comprehended in accounting control may also be involved in administrative control. For example, sales and cost records classified by products may be used for accounting control purposes and also in making management decisions concerning unit prices or other aspects of operations. Such multiple uses of procedures or records, however, are not critical because they are concerned primarily with clarifying the outer boundary of accounting control. Examples of records used solely for administrative control are those pertaining to customers contacted by salesmen and to defective work by production employees maintained only for evaluation personnel per performance.

These earlier AICPA standards stressed that the system of internal control extends beyond matters relating directly to the accounting and financial statements but also that the primary interest for purposes of the financial statements is with their internal accounting control. These standards specifically state that accounting control is within the scope of the study and evaluation of internal control, but administrative control is not. In those earlier days, the evolving information systems consisting of early computers and unit record accounting machines was considered an administrative control matter.

The persons involved with internal controls in organizations included the external and internal auditors, financial management, and for automated financial systems, information systems professionals. Although their perspectives differed, each of these groups have always been interested in the effectiveness of the total system of internal control beyond just internal accounting control. Concerned with the integrity of the systems they were developing and implementing, information systems professionals have generally believed that internal accounting control was part of a larger control system but with the lines of demarcation where internal accounting control fits in the total system never exactly clear. As a result, authoritative interpretations of internal control were published by both the United States Securities and Exchange Commission (SEC) and the AICPA as well as voluminous guidelines developed by major public accounting firms.

For information systems professionals, the concept of internal control go back to concerns of the correctness of batch oriented transaction systems and concerns over physical security. Many earlier control systems were designed to monitor the number of items input and to tie that number to the number accepted plus the number rejected. With the large investments required for legacy mainframe systems and with the terrorism and unrest, particularly in the 1970s, many considered control in terms of physical security controls.

The definition of internal control has changed and evolved, and while the older interpretations are not incorrect, they have been expanded and clarified since 1992, and it is useful to understand the historical evolution of these definitions.

3. THE FOREIGN CORRUPT PRACTICES ACT OF 1977

The period of 1974 through 1977 was a time of extreme social and political turmoil in the United States. The 1972 presidential election was surrounded by allegations of a series of illegal and questionable acts that eventually led to the U.S. President's resignation. The events were first precipitated by a burglary of the Democratic party headquarters then located in a building complex known as Watergate. The resulting scandal and related investigations became known as the "Watergate" affair. Investigators found, among other matters, that various bribes and other questionable practices had occurred that were not covered by legislation.

In 1976, the SEC submitted to the U.S. Senate Committee on Banking, Housing, and Urban Affairs a report on its "Watergate" related investigations into various questionable or potentially illegal corporate payments and practices. The phrase "potentially illegal" is used because many legal statutes in place at the time were somewhat vague regarding these activities. The Senate report recommended Federal legislation to prohibit these bribes and other questionable payments. In response to the report's recommendation, the Foreign Corrupt Practices Act (FCPA) was enacted in December 1977. The act contains provisions requiring the maintenance of accurate books and records, systems of internal accounting control, and prohibitions against bribery. The FCPA provisions apply to virtually all U.S. companies with SEC registered securities. Using terminology taken directly from the Act, SEC regulated organizations must:

- Make and keep books, records, and accounts, which, in reasonable detail, accurately and fairly reflect the transactions and dispositions of the assets of the issuers.
- Devise and maintain a system of internal accounting controls sufficient to provide reasonable assurances that:
  - Transactions are executed in accordance with management's general or specific authorization;
  - Transactions are recorded as necessary both to permit the preparation of financial statements in conformity with generally accepted accounting principles or any other criteria applicable to such statements, and also to maintain accountability for assets;
  - Access to assets is permitted only in accordance with management's general or specific authorization, and
  - The recorded accountability for assets is compared with the existing assets at reasonable intervals, and appropriate action is taken with respect to any differences.

The special significance of FCPA requirements was that for first time management was made responsible for having an adequate system of internal accounting control. This responsibility overlapped with, but went beyond, the external auditors' reliance on just internal accounting control to support an opinion on the fairness of the financial statements of the organization. However, it was significant that the FCPA requirements used word-for-word the AICPA's internal control definition.

The FCPA requires organizations to "make and keep books, records, and accounts, which in reasonable detail, accurately and fairly reflect the transactions and dispositions of the assets of the issuer." This provision applies to organizations that have securities that are SEC registered and does not apply to nonpublic companies. The FCPA requires that records are kept accurately and in reasonable detail to reflect supporting transactions. The phase "in reasonable detail" was added to address concerns that no accounting system could achieve complete freedom from error. While there is no exact definition of "in reasonable detail," the intent of the rule appears that records should reflect transactions in conformity with accepted

methods of recording economic events, preventing off the books "slush funds" and payments of bribes.

The FCPA also requires that companies with registered securities maintain a system of "internal accounting controls." These controls should be sufficient to provide reasonable assurances that transactions are authorized and recorded to permit preparation of financial statements in conformity with generally accepted accounting principles. Accountability is to be maintained for assets and access to the assets permitted only as authorized. Also per the statute, recorded assets are to be physically inventoried periodically with significant differences analyzed.

Because the cost for fully controlling each organization transaction can not be justified in the face of existing risks, the act uses the term 'reasonable assurances' when mandating accounting control requirements. Management must estimate and evaluate these cost versus benefit relationships and judge the appropriate steps to be taken.

The FCPA makes no specific references information systems; automated systems were evidently considered to be just another form or format of record that must be maintained.

The Act suggests that various groups may be involved in determining an organization's compliance with FCPA standards. The controller or vice president of finance would be responsible for the financial control system. External auditors are involved through reviewing management's representations of its control system. Legal counsel would be interested because of the need for interpretations of compliance with the Act. Internal audit, of course, would be involved because of its responsibilities for the evaluation of internal control. Because of the FCPA, the boards of directors and their audit committees in many companies began to take an active part in directing reviews of internal controls. Although these activities were initiated to assure compliance with the FCPA, they have continued because of a general management recognition of the importance of good internal controls.

When enacted, the FCPA resulted in a flurry of activity among major U.S. corporations. In the years immediately following its enactment, many organizations initiated major efforts to assess and document their systems of internal control. Organizations that had never formally documented procedures, embarked on major documentation efforts. This responsibility for FCPA documentation was usually given to internal audit departments who used their best efforts to comply with the internal control provisions of the Act. However, unless the organization had a strong information systems audit capability, technical or computer systems documentation was often limited at best. Considerable efforts were expended in these efforts, and many consultants and seminar presenters became wealthier in the process. Even though systems and procedures change over relatively short periods of time, many large organizations developed extensive sets of paper based documentation with no provisions, once they had been completed, to update them.

Many anticipated a wave of additional regulations or legal initiatives following the enactment of the FCPA. However, this did not occur. Legal actions were relatively minor, no one came looking for the files of assembled documentation, and the FCPA dropped off of the list of current, "hot" management topics. The FCPA is still in force, a U.S. law requiring corporate compliance. The FCPA did emphasize the importance of internal control and many initiatives then were launched to improve internal control evaluations in the modern organization.

4. THE TREADWAY COMMISSION AND THE ORIGINS OF COSO

With all of the various published approaches for understanding and documenting internal controls, it soon became obvious to the accounting profession that the various parties involved in this FCPA documentation process, including business and financial managers, did not have a clear and consistent understanding of what was meant by the term "internal control." As discussed previously, external auditors thought in terms of "internal *accounting* control" while internal auditors had their own broader definition of internal control. Information systems professionals thought of control primarily in terms of input and output controls, the number of line of output or lines reported by a program must relate to a count for the number of inputs.

Concurrent with these internal control definition differences, the financial press and others in the U.S. began to discuss the need for external auditors to express an opinion on an organization's internal controls as part of their audits of financial statements. At that time, in the later 1970s, external auditors merely reported than an organization's financial statements were "fairly presented." There was no attention given to, or any mention made of, the internal control procedures supporting those financial statements. The FCPA required organizations to document their internal controls but did not ask independent public accountants to attest to whether the organizations under audit were in compliance with any internal control reporting requirements. The SEC, which regulates publicly held companies in the United States, began to study whether external audit reports were adequate. As a result, a series of studies and reports were completed over about a ten-year period in the United States to define better both internal control as well as the external auditor's responsibility for reporting on the adequacy of those controls.

First, the AICPA formed a high-level Commission on Auditors' Responsibilities in 1974 to study the issue of the external auditor's responsibility for reporting on internal controls. This group, better known then as the Cohen Commission, released its report in 1978 recommending that corporate management present a statement on the condition of the company's internal controls along with the financial statements. These Cohen Commission initiatives were taking place concurrently with the development and initial publication of the FCPA. At about the same time, the CICA's Commission on Auditor Expectations released a report in 1978 with similar conditions.

In the United States, the Cohen Commission's report initially ran into a torrent of criticism. In particular, the report's recommendations were not precise on what was meant by "reporting on internal controls", and external auditors expressed concerns about their roles in this reporting process. They were concerned about potential liabilities if their reports on internal control gave inconsistent signals due to a lack of understanding over what were internal control standards. Although outside auditors were accustomed to attesting to the fairness of financial statements, the Cohen Commission report suggested that they should express an audit opinion on the fairness of management's assertions in a proposed internal control letter. One of the issues raised was that management did not have a consistent definition of internal control. Organizations might use similar terms to describe the quality of their internal controls with each meaning something a little different. If an organization reported that its controls were "adequate" and if the auditors "blessed" the assertions in that controls report, the external auditors could later be criticized or even suffer potential litigation if some significant control problem appeared at a later date.

The Financial Executives Institute (FEI) got involved in this internal controls reporting controversy during the same period. Just as the AICPA or CICA represents the public accountants in the United States or Canada, respectively, the FEI represents senior financial officers in organizations. The FEI released a letter to its members in the late 1970s endorsing the Cohen Commission's recommendations on internal control reports. They suggested that publicly held organizations should report on the status of their internal accounting controls, but they provided no detail as to what was meant by internal accounting controls. Again, there no mention of any information systems control issues.

As a result these various recommendations, publicly held corporations in the United States began to discuss the adequacy of their internal controls as part of the management letters included in annual reports. These internal control letters were not required and those issued did not follow any standard format. They typically included comments stating that management, through its internal auditors, periodically assessed the quality of its internal controls. The same letters sometimes included "negative assurance" comments indicating that nothing was found by internal auditors to indicate that their might be an internal control problem in the organization's operations.

This term "negative assurance" will return again in the discussion of internal controls. Because an external auditor can not detect all problems and because of the risk of potential litigation, external audit reports often have been stated in terms of a negative assurance. That is, rather than saying that they "found no problems" in an area under review, they have tended to report that they did not find anything that would lead them to believe that there was a problem. This is a subtle but important difference.

Based on the Cohen Commission and the FEI's recommendations, the SEC issued proposed rules calling for *mandatory* management reports on an entity's internal

accounting control system. The SEC suggested that information on the effectiveness of an entity's internal control system *was necessary* to allow investors to evaluate better both management's performance and the integrity of published financial reports.

The SEC proposal raised a storm of controversy. First, many senior managers felt that this was an onerous requirement on top of the new released FCPA regulations. Questions were once again raised regarding the definition of internal accounting control, and while organizations might agree to voluntary reporting, they did not want to subject themselves to the civil and legal penalties associated with a violation of SEC regulations.

The SEC soon dropped this 1979 internal control reporting proposal, but they promised to re-release the regulations at a later date. The SEC proposal was important, however, in that it emphasized the need for a separate management report on internal accounting controls as part of the annual report to shareholders and the required SEC filings. This tentative regulation caused larger public companies to issue voluntary internal control comments or letters in their annual reports.

In parallel with the SEC's proposed rules on internal control reporting, the AICPA formed another committee, the Special Advisory Committee on Internal Control, or the Minahan Committee. Their concluding 1979 report pointed out the lack of management guidance on internal control procedures and acknowledged that most of the published guidance on internal controls was only found in the accounting and auditing literature. This guidance would not necessarily come to the attention or, be completely relevant to, a business or information systems manager with who had a need to understand internal control concepts.

At about the same time, the FEI Research Foundation (FERF) commissioned studies in this area that concluded the definitions used by various professional standards setting groups defining the characteristics, conditions, practices and procedures of internal control systems had vast differences in what constitutes an effective system of internal control. Because of the need for a better and more consistent definition of internal controls, regulatory authorities could not realistically draft requirements for reporting on internal control.

The AICPA's definition of internal control is of special interest because it supports the external auditor's expression of an opinion as to the fairness of the financial statements. The AICPA's standards are defined through a series of Statements on Auditing Standards (SASs) that are released from time to time and are also codified in an overall set of professional standards. While these standards were once almost "engraved in stone" with little change for many years, during the 1970s and 1980s, the public accounting profession was faced with criticism that its standards did not provide adequate guidance. This problem was called the "expectations gap," because public accounting standards did not meet the expectations of investors in the area of internal control and other matters. To answer this need the AICPA

released a series of new SASs on internal control including SAS No. 48, *The Effects of Computer Processing on the Examination of Financial Statements,* 1984, that provide guidance on the need to review both the computer systems applications controls as well as general controls, such as physical security. Although there had been massive technological changes in the way computer systems are constructed, at the time SAS No. 48 was issued external auditors were still using guidance from the early 1970s.

Shortly after SAS No. 48, the AICPA released SAS No. 55, *Consideration of the Internal Control Structure in a Financial Statement Audit,* 1988, that defined internal control in terms of an entity's overall *control structure,* consisting of three elements: (1) the control environment, (2) the accounting system, and (3) control procedures.

SAS No 55 presented a somewhat different approach to understanding internal control than had been used by the AICPA in the past as well as by other standards setting groups, such as the Institute of Internal Auditors. It also looked at information systems controls as a specialized but important portion of the overall control structure. SAS No. 55 got rid of the older, legacy system concept of information systems controls which emphasized such areas as physical security but give little attention to application control procedures.

An organization generally has other internal control structure policies and procedures that are not relevant to a financial statement audit and therefore are not considered by the external auditors. Examples include policies and procedures concerning the effectiveness, economy, and efficiency of certain management decision-making processes, such as setting of an appropriate price for products or deciding whether to make expenditures for a new computer system. Although these processes are certainly important to the organization, they do not ordinarily relate to the external auditor's financial statement audit.

5. TREADWAY COMMITTEE REPORT

The same period of the later 1970s and early 80s saw many major company failures in the United States due to factors such as high inflation, the resultant high interest rates, and high energy costs because of excessive government regulation. Organizations sometimes reported adequate earnings in their financial reports, and their external auditors attested that these same financial reports were "fairly stated," only to have the organization suffer a financial collapse shortly after the release of the audited reports. While some of these failures were caused by fraudulent financial reporting, many were due to high inflation or other factors causing organization instability. Several members of Congress proposed legislation to "correct" these potential business and audit failures. Bills were drafted, Congressional hearings held, many solutions were suggested, but no legislation was passed.

Also in response to these concerns, the National Commission on Fraudulent Financial Reporting was formed by five professional organizations: the IIA, the AICPA, and the FEI, all mentioned previously, as well as the American Accounting Association (AAA) and the Institute of Management Accountants (IMA). The AAA is a U.S. academic accountants organization, and the IMA is the professional organization for cost accountants. The National Commission on Fraudulent Reporting, called the Treadway Commission after its chairperson, had a major objective to identify casual factors that allowed fraudulent financial reporting and to make recommendations to reduce their incidence. The Treadway Commission's final report Treadway, 1987) included recommendation to management, boards of directors of public companies, the public accounting profession, and others.

The Treadway Commission report again called for management reports on the effectiveness of their internal control systems. It emphasized some key elements in what it felt should be an effective system of internal control, including a strong control environment, codes of conduct, a competent and involved audit committee, and a strong internal audit function. Nothing was mentioned concerning information systems. The Treadway Commission report again pointed out the lack of a consistent definition of internal control, suggesting further work was needed. The same organizations that managed the Treadway report, the Committee of Sponsoring Organizations (COSO), then contracted with outside specialists and embarked on a new project to define internal control. Although it defined no standards, the Treadway report was important as it raised the level of concern and attention regarding reporting on internal control. The report concluded with a recommendation that a better and more consistent definition of internal control was needed.

6. THE COSO MODEL OF INTERNAL CONTROL

The "Sponsoring Organizations" in the COSO name are the five professional auditing and accounting organizations that developed this internal control report. The COSO report is its commonly accepted name. The sponsoring organizations contracted with the public accounting firm of Coopers and Lybrand to manage the development of the actual report, and a large number of volunteers helped to research issues and develop the final report. The COSO development group first released a draft report in 1990 for public exposure and comment. More than 40,000 copies of this draft version were sent to corporate officers, internal and external auditors, legislators, academics, and other interested parties. Formal comments regarding this draft were requested, and based on comments received, a revised draft was circulated a more limited group for additional comment. In addition, the internal control review procedures portion of the study, discussed later, was field tested by five public accounting firms.

The final COSO report was released in September 1992. The report proposes a common framework for the definition of internal control as well as procedures to evaluate those controls. While the report does not have the authority of a standards-

setting document, such as an AICPA auditing standard (SAS) or a government agency regulation, all significant parties involved in the process of evaluating internal control standards have endorsed the COSO report and its internal control framework definition. For example, the AICPA has modified its internal control standards through SAS No. 78 to bring them in compliance with the COSO model of internal control. The report has also been used to develop new laws and regulations such as the Federal Deposit Insurance Corporation Improvement Act of 1991 (FIDICIA), that contains regulations for larger banks. The 1993 regulations for FIDICIA used the COSO definition of internal control with no modifications.

The COSO report recognizes the role of information systems in the overall control structure. This is almost a "first" for organization internal control standards. Rather than highlighting on physical security general controls or "do the debits equal the credits?" types of application controls, COSO talks about such things as the importance of highly integrated information systems and the need for strategic systems planning.

The COSO report introduced a good description of the multidimensional concept of internal control, defining internal control as follows:

> Internal control is a *process,* effected by an entity's board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories:
>
> - Effectiveness and efficiency of operations
> - Reliability of financial reporting
> - Compliance with Applicable laws and regulations.

This is the *official* COSO report definition of internal control. COSO report uses diagrams to describe a three-dimensional view of the internal control system in an organization. The horizontal levels describe the components of internal control as:

- The Control Environment
- Risk Assessment
- Control Activities
- Information and Communications
- Monitoring

Vertical segments along the "y" axis are the three components on internal control discussed previously, financial reporting, compliance, and effectiveness and efficiency of operations. The third dimension of internal control is found along the "z" axis and can consist of many segments, each representing a unit or activity of the organization to which internal control relates.

Another, perhaps better way to view the COSO model is a cube. Alternatively, this model is shown as a pyramid where the Control Environment forms the foundation of the internal control model with Monitoring, often by senior management, as a smaller component at the top of the pyramid. One component, Information and

Communication, is not a separate layer but is used to connect all of the other components of internal control. This is where information systems fits in this structure.

The three COSO internal control objectives, effectiveness of operations, reliability of financial reporting, and compliance with laws and regulations, again appear as components of internal control running from the foundation Control Environment to Monitoring as the apex. The third dimension to this model are the units or activities of the entity to which this internal control system relates. The number or type of these activities or units may vary from one organization to another.

The objective of this paper is not to describe the COSO internal control model in any level of detail. The previously referenced COSO report describes this. However, the Information and Communication component is of particular importance to the information systems professional. This component is not a horizontal layer, but it spans across all of the other internal control components just as the information systems function in the modern organization has an influence throughout the organization.

Information and communications are related but really very distinct internal control components of the internal control framework. Appropriate information must be communicated up and down through the organization in a manner and time frame that allow people to carry out their various responsibilities. These information flows are supported by automated systems. In addition to formal and informal communication systems, organizations must have effective procedures in place to disseminate communication.

7. COSO AND INFORMATION SYSTEMS CONTROLS

Various types of information, and their supporting automated systems, are needed at all levels to achieve organizational operational, financial reporting, and compliance objectives. The organization, for example, needs proper information in order to prepare the financial reports that are communicated to outside investors. It also needs both internal cost information and external market preference information in order to make correct marketing decisions. This information must flow both from the top levels of the organization on down and upward from lower levels. COSO takes a very broad approach to the concept of an information system. The report recognizes the importance of automated systems but makes the point that information systems can be manual, automated, or conceptual. Any of these information systems can be either formal or informal.

Differing from financial control type of standards, the COSO report emphasizes the importance of systems integrity and keeping its information systems consistent with overall organization needs. Information systems must change to support changes on many levels, but frequently an information system implemented many years ago

had objectives to support very different needs. Although its application controls may be good, that older information system may not support the current needs of the organization.

Accounting and financial processes were the first automated system in organizations, starting with the unit record or "IBM card" accounting machines in the 1950s and then moving to the earliest computer systems. Some organizations may have upgraded their automated systems over time with the introduction of new computer technologies, but their basic mix of supporting automated systems has not changed significantly. An organization still may have its general ledger, payroll, inventory, accounts receivable, accounts payable, and related financial based processes as their core information systems without too much else. The COSO report suggests that the effective organization should go a step further and implement both strategic and integrated information systems.

By a strategic system, the report suggests that management should consider the planning, design, and implementation of its information systems as part of its overall organization strategy. These strategic systems then support the organization's overall business and help it to carry out its overall business missions. There have been many examples of companies that developed strategic information systems to support their business strategies that moved them even further forward. An example might be American Airlines that developed its SABRE automated reservation system in the 1960s, greatly enhancing its ability to sell tickets and make more effective use of its resources. Subsequently, American developed the first frequent flyer program in the early 1980s, again giving it a business edge. Other airlines subsequently developed similar or even better information systems, but American Airlines initial systems gave them an initial marketing and customer acceptance edge for a time.

The effective organization should develop strategic information systems, whether automated or even manual. Not every organization has the resources or needs to develop systems in the nature of scale of SABRE; however, even smaller systems should be designed and developed to support the organization's strategies. These strategic systems will allow organizations to understand and to respond better to changes in their marketplaces and control environments.

These comments about strategic information systems are a step into the future when contrasted with the information systems related comments from earlier internal control standards. COSO makes the point, however, that it is a mistake to assume that just because a system is new it will provide better control. Older systems have presumably been tried and tested through use while the new system can have unknown or untested control weaknesses.

Closely related to systems integrity, COSO discusses the importance of the quality of information. Poor quality information systems, filled with errors and omissions, affect management's ability to make appropriate decisions. Reports should contain

enough data and information to support effective control activities. The COSO report points out that this concept quality of information includes ascertaining whether:

- The content of reported information is appropriate,
- The information is timely and available when required,
- The information is current or at least the latest available,
- The data and information are correct, and
- The information is accessible to appropriate parties.

These points all mention issues that should be covered in overall good systems design. If an information system does not meet these quality issues, it is possible that the system will not meet management requirements. The comments push the COSO standard beyond that of just internal control to that of almost a quality standard.

8. THE COSO INTERNAL CONTROL FRAMEWORK

The COSO internal control framework is a much more complex module than has been described in earlier, pre-COSO internal control definitions. Here, internal control is described in terms of a three-dimensional model with separate and independent x-, y-, and z- axes components. The internal control components are the horizontal layers on the y-scale. The three internal control objectives, financial reporting, operations, and compliance with laws and regulations lay on the x-axis and divide the model with vertical lines. Finally, the z-axis divides the model into the separate activities and entities in the organization. The internal control structure for any area in the organization can be separately viewed using this three-dimensional model, and information systems controls can be viewed within this same context.

This model might allow the information systems professional to think it possible to focus on just the internal control structure for one component such as a specialized tracking system. Internal control, however, is not that simple, and each element must be considered with respect to all of the other components in the total framework.

This narrow view of looking at only one element caused the failure of earlier approaches for evaluating internal controls. A manager or information systems professional might have looked at financial accounting controls and procedures for some independent Division A of an organization with little attention paid to the other related components including the control environment or risk-assessment issues, or to other entities in the total organization such as other Divisions or operating units. This narrow view sometimes caused internal control evaluators to miss significant, interrelated internal control issues.

The COSO report provides an excellent description of the components of an internal control framework as well as an integrated model that ties these components together. Management should always keep this broad picture of internal control.

The COSO report concludes with comments that internal control can only provide reasonable but not absolute assurance that an organization will achieve its objectives. For example, an on-line purchasing system, handling international contracts, can have good controls in place to provide assurance that the system is in compliance with significant import laws and regulations. A determined rogue employee, however, might be able to get around those controls and cause the violation of some significant regulation. While procedures can be improved to prevent this from happening again, it is very difficult to make control totally fault free.

These inherent internal control limitations make the role of internal control evaluation even more important in the modern organization. Good internal controls will only provide *reasonable assurance* that the entity will achieve its objectives. The COSO report reminds readers that, "Internal control is not a panacea." These are rather strong words, but the report tries to emphasize that management should not operate under the false assurance that because its internal controls are good, it will not be face any significant risks or exposures. Internal control, no matter how effective, will operate somewhat differently with respect to each of the established control objectives.

9. FUTURE INTERNAL CONTROL AND INTEGRITY ISSUES

While COSO was just a report by a non-authoritative body, its internal control model is now beginning to be incorporated in other standards in the United States. For example, the American Institute of Certified Public Accountants released in 1996 their Statement on Auditing Standards No. 78 , requiring external auditors after 1997 to essentially consider the COSO model of internal control when expressing their opinions on the fairness of financial statements. This COSO model has been incorporated elsewhere including Canadian accounting standards and in some United States governmental regulations. However, although the COSO report emphasizes the importance of information systems in its internal control model, little attention has been given to COSO defined information systems controls by either the auditors or information systems professionals. Within the U.S., there will probably much more emphasis given to the SAS No. 78 related COSO standards once the become official, once the AICPA issues a more detailed audit guide type of book covering the standard, and most importantly, once the major public accounting firms issue detailed guidance covering the this new auditing standard.

Canada is developing internal control auditing standards very similar to the COSO model, and because so many organizations worldwide are subject to AICPA auditing and United States financial reporting standards, the COSO model can be

expected to have a worldwide impact over time. However, not all may be implementing consistent standards. Other audit standards setting groups, the IIA in particular, are incorporating COSO controls in their internal audit standards.

This COSO model does not have the same level or recognition in the information systems world. For example, a search for references to "COSO" in the IEEE Computer Society's publication Computer, for the years 1994 to the present identified no hits. Similarly, a search for "internal control" in that same period yielded only three references, and those only notices using the word in the Call for Papers section. Other searches or this same period proved equally fruitless. Internet Web browser engine driven searches found essentially no references tot the above two keywords except auditing organization related materials, government agency regulations, and college course descriptions.

The literature covering information systems is vast, but the software engines allowing searches for specific topics is limited. The comment is made despite the fact that much literature is available on the Internet and can be reached through keyword searches. Searches for references to information systems controls and even systems integrity yielded few meaningful references. There are numerous references to "integrity," but most are in the context of systems reliability and not internal control integrity. It would appear that there is a fairly wide gap in computing literature in these areas. While information systems professionals are interested in building systems with adequate controls, this is no longer a "hot topic" for the information systems professional. The concepts and spirit behind the COSO internal control model evidently have not been communicated to information systems professionals.

While topics can not be as easily searched through Internet type mechanisms, there is a vast number of books published every year on information systems related topics. While certainly not an all inclusive search, we looked at two relatively recent U.S. market books on building quality systems, Glass (1992) and Bochenski (1994) and one with a more European perspective, Ciborra and Jelassi (1994). While each addresses the concepts of quality and reliable software, neither the terms "internal control" nor "integrity" are referenced in any of these books' indexes. It would almost appear that these terms have moved out to the computing literature.

The gap here is interesting. While the COSO model allowing auditing and accounting professionals to take a big step beyond a narrow "Do the debits equal the credits?" internal control approach, it would appear that more attention is needed in the information systems community to build systems covering the comprehensive COSO controls model approach.

Over time, the COSO model of internal controls will probably be given much more attention by auditors on a worldwide basis as well as by supporting managers. The model provides a broader, more integrated picture of internal control than the

earlier concepts sued by auditors. There appears to be an excellent model for looking at and developing information systems with good integrity controls. More efforts are needed in communicating this COSO concept to the information system community.

10. REFERENCES

American Institute of Certified Public Accountants, Statement on Auditing Standards No. 1, New York

American Institute of Certified Public Accountants, Statement on Auditing Standards No. 78, New York

Bobhenski, B. (1994) Implementing Production-Quality Client/Server Systems, John Wiley, New York

Brink, V. Z. (1942) Modern Internal Auditing, John Wiley, New York

Ciborra, C. & Jelassi, T. eds. (1994) Strategic Information Systems: A European Perspective, John Wiley, Chichester, England

Committee of the Sponsoring Organizations (COSO) of the Treadway Commission. (1992) Internal Control -- Integrated Framework. New York

Glass, R. L. (1992), Building Quality Software, Prentice Hall, Englewood Cliffs, NJ

11. BIOGRAPHY

Robert Moeller is president of Compliance and Control Systems Associates, Inc., a Chicago, IL based consulting and seminar delivery organization. He previously was Audit Director for Sears Roebuck and National Director of Computer Auditing for Grant Thornton. Mr. Moeller has a bachelors degree in aeronautical engineering from the University of Minnesota and a MBA in finance from the University of Chicago. The author of two books, his professional activities include previously chairing the AICPA's Computer Audit Subcommittee and IFIP TC-11 WG 11.5.