

Complements of:

THE BONADIO GROUP
Business Consulting & More

171 Sully's Trail
Pittsford, NY 14450
(585) 381-1000

**A Comparison of Internal Controls:
COBIT®, SAC, COSO and SAS 55/78**

By Janet L. Colbert, Ph.D., CPA, CIA, and Paul
L. Bowen, Ph.D., CPA

In recent years, increased attention has been devoted to internal control by auditors, managers, accountants, and legislators. Five recently issued documents are the result of continuing efforts to

define, assess, report on, and improve internal control. They are: the Information Systems Audit and Control Foundation's COBIT (Control Objectives for Information and related Technology), the Institute of Internal Auditors Research Foundation's Systems Auditability and Control (SAC), the Committee of Sponsoring Organizations of the Treadway Commission's Internal Control - Integrated Framework (COSO), and the American Institute of Certified Public Accountants' Consideration of the Internal Control Structure in a Financial Statement Audit (SAS 55), as amended by Consideration of Internal Control in a Financial Statement Audit: An Amendment to SAS 55 (SAS 78).

COBIT (1996) is a framework providing a tool for business process owners to efficiently and effectively discharge their IS control responsibilities. SAC (1991, revised 1994) offers assistance to internal auditors on the control and audit of information systems and technology. COSO (1992) makes recommendations to management on how to evaluate, report, and improve control systems. SASs 55 (1988b) and 78 (1995) provide guidance to external auditors regarding the impact of internal control on planning and performing an audit of an organization's financial statements.

Because different bodies developed the documents to address the specific needs of their own audiences, some disparities may exist. Nevertheless, each document focuses on internal control and each audience, i.e., internal auditors, management, and external auditors, devotes much time and effort toward establishing or evaluating internal controls. Therefore, comparing the internal control concepts presented in these documents is of interest to members of all three audiences.

A comparison of the five documents reveals that each builds on the contributions of the previous documents. COBIT incorporates as part of its source documents both COSO and SAC. It takes its definition of control from COSO and its definition of IT Control Objectives from SAC. SAC embodies the internal control concepts developed in SAS 55, COSO uses the internal control concepts in both SAS 55 and SAC, and SAS 78 amends SAS 55 to reflect the contributions to internal control concepts made by COSO. In particular, SAS 78 responds to the Winters and Guy (1992) call for a reconciliation of the internal control concepts presented in the COSO report and SAS 55.

This article summarizes the four documents (SAC 55/78 are combined.) and compares the internal control concepts presented in each. The following Table notes the major issues presented.

Comparison of Control Concepts

	COBIT	SAC	COSO	SASs 55/78
Primary Audience	Management, users, information system auditors	Internal Auditors	Management	External Auditors
IC viewed as a	Set of processes including policies, procedures, practices, and organizational structures	Set of processes, subsystems, and people	Process	Process
IC Objectives organizational	Effective & efficient operations Confidentiality, Integrity and availability of information Reliable financial reporting Compliance with laws & regs	Effective & efficient operations Reliable financial reporting Compliance with laws & regs	Effective & efficient operations Reliable financial reporting Compliance with laws & regs	Reliable financial reporting Effective & efficient operations Compliance with laws & regs
Components or Domains	Domains: Planning and organization Acquisition and implementation Delivery and support Monitoring	Components: Control Environment Manual & Automated Systems Control Procedures	Components: Control Environment Risk Management Control Activities Information & Communication Monitoring	Components: Control Environment Risk Assessment Control Activities Information & Communication Monitoring
Focus	Information Technology	Information Technology	Overall Entity	Financial Statement
IC Effectiveness Evaluated	For a period of time	For a period of time	At a point in time	For a period of time
Responsibility for IC System	Management	Management	Management	Management
Size	187 pages in four documents	1193 pages in 12 modules	353 pages in four volumes	63 pages in two documents

Summaries of the Documents

COBIT: Control Objectives for Information and related Technology

The Information Systems Audit and Control Foundation (ISACF) recently developed the Control Objectives for Information and related Technology (COBIT) to serve as a framework of generally applicable and IS security and control practices for information technology control. (The report can be ordered from ISACA by phone or mail.) This COBIT framework allows management to benchmark the security and control practices of IT environments, allows users of IT services to be assured that adequate security and control exists, and

allows auditors to substantiate their opinions on internal control and to advise on IT security and control matters. The primary motivation for providing this framework was to enable the development of clear policy and good practices for IT control throughout industry worldwide.

The completed phase of the COBIT project provides an *Executive Summary*, a *Framework* for control of IT, a list of *Control Objectives*, and a set of *Audit Guidelines*. (The control objectives and audit guidelines are referenced to the framework.)

Future phases of the project will provide self-assessment guidelines for management and identify new or updated control objectives through incorporations of other identified global control standards. Plus, add control guidelines and identify key performance indicators.

Definition: COBIT adapted its definition of control from COSO: The policies, procedures, practices, and organizational structures are designed to provide reasonable assurance that business objectives will be achieved and that undesired events will be prevented or detected and corrected.

COBIT adapts its definition of an IT control objective from SAC: A statement of the desired result or purpose to be achieved by implementing control procedures in a particular IT activity.

COBIT emphasizes the role and impact of IT control as they relate to business processes. The document outlines platform and application independent IT control objectives.

IT Resources: COBIT classifies IT resources as data, application systems, technology, facilities, and people. Data is defined in its widest sense and includes not only numbers, text, and dates but objects such as graphics and sound. Application systems are understood to be the sum of manual and programmed procedures.

Technology refers to hardware, operating systems, networking equipment, and the like. Facilities are the resources used to house and support information systems. People addresses individuals' skills and abilities to plan, organize, acquire, deliver, support, and monitor information systems and services.

Requirements: To satisfy business objectives, information needs to conform to certain criteria which COBIT refers to as business requirements for information. COBIT combines the principles embedded in existing reference models in three broad categories: quality, fiduciary responsibility and security. From these broad requirements, the report extracts seven overlapping categories of criteria for evaluating how well IT resources are meeting business requirements for information. These criteria are effectiveness, efficiency, confidentiality, integrity, availability, compliance, and reliability of information.

Process and Domains: Based on analysis of the information technology infrastructure library (ITIL) IT management practices, a UK document, COBIT classifies IT processes into four domains. These four domains are (1) planning and organization, (2) acquisition and implementation, (3) delivery and support and (4) monitoring. The natural grouping of processes into domains is often confirmed as responsibility domains in an organizational structure and follows the management cycle or life cycle applicable to IT processes in any IT environment. The Exhibit illustrates the relationship between IT resources and the four IT process domains and lists 32 individual IT processes within the four domains.

COBIT presents a framework of control for business process owners. Increasingly, management is fully empowered with complete responsibility and authority for business processes. COBIT includes definitions of both internal control and IT control objectives, four domains of processes and 32 high level control statements for those processes, 271 control objectives referenced to those 32 processes and audit guidelines linked to the control objectives.

Framework: The COBIT framework provides high-level control statements for particular IT processes. The framework identifies the business need satisfied by the control statement, identifies the IT resources managed by the processes, states the enabling controls and lists the major applicable control objectives.

SAC Report

The SAC report defines the system of internal control, describes its components, provides several classifications of controls, describes control objectives and risks, and defines the internal auditor's role. The

report provides guidance on using, managing, and protecting information technology resources and discusses the effects of end-user computing, telecommunications, and emerging technologies.

Definition: The SAC report defines a system of internal control as: a set of processes, functions, activities, subsystems, and people who are grouped together or consciously segregated to ensure the effective achievement of objectives and goals.

The report emphasizes the role and impact of computerized information systems on the system of internal controls. It stresses the need to assess risks, to weigh costs and benefits, and to build controls into systems rather than add them after implementation.

Components: The system of internal control consists of three components: the control environment, manual and automated systems, and control procedures. The control environment includes organization structure, control framework, policies and procedures, and external influences. Automated systems consist of systems and application software. SAC discusses the control risks associated with end-user and departmental systems but neither describes nor defines manual systems. Control procedures consist of general, application, and compensating controls.

Classifications: SAC provides five classification schemes for internal controls in information systems: (1) preventive, detective, and corrective, (2) discretionary and non-discretionary, (3) voluntary and mandated, (4) manual and automated, and (5) application and general controls. These schemes focus on when the control is applied, whether the control can be bypassed, who imposes the need for the control, how the control is implemented, and where in the software the control is implemented.

Control Objectives and Risks: Risks include fraud, errors, business interruptions, and inefficient and ineffective use of resources. Control objectives reduce these risks and assure information integrity, security, and compliance. Information integrity is guarded by input, processing, output, and software quality controls. Security measures include data, physical, and program security controls. Compliance controls ensure conformance with laws and regulations, accounting and auditing standards, and internal policies and procedures.

Internal Auditor's Role: Responsibilities of internal auditors include ensuring the adequacy of the system of internal control, the reliability of data, and the efficient use of the organization's resources. Internal auditors are also concerned with preventing and detecting fraud, and coordinating activities with external auditors. The integration of audit and information system skills and an understanding of the impact of information technology on the audit process are necessary for internal auditors. These professionals now perform financial, operational and information systems audits.

COSO Report

The COSO report defines internal control, describes its components, and provides criteria against which control systems can be evaluated. The report offers guidance for public reporting on internal control and provides materials that management, auditors, and others can use to evaluate an internal control system. Two major goals of the report are to (1) establish a common definition of internal control that serves many different parties, and (2) provide a standard against which organizations can assess their control systems and determine how to improve them.

Definition: The COSO report defines internal control as: 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.

The report emphasizes that the internal control system is a tool of, but not a substitute for, management and that controls should be built into, rather than built onto, operating activities. Although the report defines internal control as a process, it recommends evaluating the effectiveness of internal control as of a point in time.

Components: The internal control system consists of five interrelated components: (1) control environment, (2) risk assessment, (3) control activities, (4) information and communication, and (5) monitoring. The control environment provides the foundation for the other components. It encompasses such factors as management's philosophy and operating style, human resource policies and practices, the integrity and ethical values of employees, the organizational structure, and the attention and direction of the board of directors. The COSO report provides guidance for evaluating each of these factors. For example, management's philosophy and operating style can be assessed by examining the nature of the business risks management accepts, the frequency of their interaction with subordinates, and their attitudes toward financial reporting.

Risk assessment consists of risk identification and risk analysis. Risk identification includes examining external factors such as technological developments, competition, and economic changes, and internal factors such as personnel quality, the nature of the entity's activities, and the characteristics of information system processing. Risk analysis involves estimating the significance of the risk, assessing the likelihood of the risk occurring, and considering how to manage the risk.

Control activities consist of the policies and procedures that ensure employees carry out management directives. Control activities include reviews of the control system, physical controls, segregation of duties, and information system controls. Controls over information systems include general controls and application controls. General controls are those covering access, software, and system development. Application controls are those which prevent errors from entering the system or detect and correct errors present in the system.

The entity obtains pertinent information and communicates it throughout the organization. The information system identifies, captures, and reports financial and operating information that is useful to control the organization's activities. Within the organization, personnel must receive the message that they must understand their roles in the internal control system, take their internal control responsibilities seriously, and, if necessary, report problems to higher levels of management. Outside the entity, individuals and organizations supplying or receiving goods or services must receive the message that the entity will not tolerate improper actions.

Management monitors the control system by reviewing the output generated by regular control activities and by conducting special evaluations. Regular control activities include comparing physical assets with recorded data, training seminars, and examinations by internal and external auditors. Special evaluations can be of varying scope and frequency. Deficiencies found during regular control activities are usually reported to the supervisor in charge; deficiencies located during special evaluations are normally communicated to higher levels of the organization.

Other Concepts: The COSO report addresses the limitations of an internal control system and the roles and responsibilities of the parties that affect a system. Limitations include faulty human judgment, misunderstanding of instructions, errors, management override, collusion, and cost versus benefit considerations.

The COSO report defines deficiencies as "conditions within an internal control system worthy of attention." Deficiencies should be reported to the person responsible for the activity and to management at least one level above the individual responsible.

An internal control system is judged to be effective if the five components are present and functioning effectively for operations, financial reporting, and compliance.

SASs 55 and 78: Statements on Auditing Standards

SASs 55 and 78 define internal control, describe its components, and provide guidance on the impact of controls when planning and performing financial statement audits.

Definition: SAS 78 replaces the definition of the internal control structure in SAS 55 with that of internal control in the COSO report except that SAS 78 emphasizes the reliability of financial reporting objective by placing it first. That is, SAS 78 defines internal control as: 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:

1. reliability of financial reporting
2. effectiveness and efficiency of operations, and
3. compliance with applicable laws and regulations.

Although SAS 78 retains the operational and compliance objectives in its definitions of internal control, SASs 55 and 78 focus on controls that affect the examination of the reliability of an entity's financial reporting. *Components:* SAS 78 replaces the three elements of the internal control structure in SAS 55, (the control environment, the accounting system, and control procedures) with the five components of the internal control system presented in COSO (control environment, risk assessment, control activities, information and communication, and monitoring).

Impact: SASs 55 and 78 require the external auditor to perform procedures to obtain a sufficient understanding of each of the five components to plan the audit. That is, the external auditor must understand the design of the entity's policies and procedures and whether the design has been placed in operation. Because they are rendering an opinion on financial statements which cover a period of time, external auditors are interested in controls affecting the capture and processing of financial information for the entire period. External auditors must report any significant internal control deficiencies that could affect financial reporting to the audit committee (SAS 60, AICPA, 1988a). At their discretion, external auditors may also communicate other control matters to the entity, e.g., opportunities to improve the accounts receivable system.

Comparison of COBIT, SAC, COSO and SASs 55/78

COBIT, SAC, COSO and SASs 55/78 define internal control, describe its components and provide evaluation tools. SAC, COSO and SASs 55/78 also suggest ways of reporting internal control problems. COBIT additionally provides a comprehensive framework facilitating analysis and communication of internal control issues. This section contrasts the contributions the individual documents make to each of these areas.

Definitions

Although the five control definitions contain essentially the same concepts, the emphases are somewhat different. COBIT views internal control as a process which includes policies, procedures, practices and organizational structures that support business processes and objectives. SAC emphasizes that internal control is a system, i.e., that internal control is a set of functions, subsystems, and people and their interrelationships. COSO accentuates internal control as a process, i.e., internal control should be an integrated part of ongoing business activities. Although they use the same definition as COSO, SASs 55/78 emphasize the reliability of financial reporting objective.

People are part of the system of internal control. COBIT classifies people (defined as staff skills, awareness and productivity to plan, organize, acquire, deliver, support and monitor information systems and services) as one of the primary resources managed by various information technology processes. The involvement of people has become more explicit as the documents have evolved. SAC explicitly identifies people as an integral part of the internal control system. COSO and SASs 55/78 note that the people involved with internal control are members of the Board of Directors, management, or other entity personnel. The documents agree that management is the party responsible for establishing, maintaining, and monitoring the system of internal control.

All four documents stress the concept of reasonable assurance as it relates to internal control. Internal control does not guarantee that the entity will achieve its objectives or even remain in business. Rather, internal control is designed to provide management with reasonable assurance regarding the achievement of objectives. The documents also acknowledge that there are inherent limitations to internal control and, because of cost/benefit considerations, not all possible controls will be implemented. Inherent limitations may cause internal controls to be less effective than planned.

In presenting the definitions of internal control, the documents assume the entity has established objectives for its operations. COBIT establishes the premise that these objectives are supported by business

processes. These processes, in turn, are supported by information provided through the use of information technology resources. Business requirements for that information only are satisfied through adequate control measures. SAC states that achieving the entity's objectives should be done effectively and stresses that objectives should be translated into measurable goals. COSO categorizes objectives as operational, financial reporting, and compliance. While SAC and COSO are concerned with objectives in all three categories, SASs 55/78 restrict their attention primarily to financial reporting objectives.

Components

The SAC report describes three components of the system of internal control. The COSO report discusses five components. SAS 78 revises SAS 55 to embrace COSO's five components. COBIT incorporates the five components discussed in the COSO report and focuses them within the information technology internal control environment. COBIT's design bridges the gap between the broader business control models such as COSO and highly technical information systems control models available worldwide. Although the documents may appear to differ in their approaches to controls, further study reveals many similarities.

Control Environment: COBIT, SAC, COSO and SAS 78 all include the control environment as a component and discuss essentially the same concepts. Factors impacting the control environment include the integrity and ethical values of management, the competence of personnel, management philosophy and operating style, how authority and responsibilities are assigned, and the guidance provided by the board of directors. COBIT weaves the implications of the control environment into all applicable control objectives. It categorizes the processes within planning and organization, acquisition and implementation, delivery and support, and monitoring. It also speaks to the control environment wherever appropriate. SAC divides the control environment into fewer categories, is more oriented to information systems, and includes ideas as part of the control environment that the other three documents discuss as part of another component. In most areas, internal control concepts develop from SAS 55 (1988) to SAC (1991, 1994) to COSO (1992) to SAS 78 (1995), to COBIT (1996). COSO and SASs 55/78 use a larger number of categories of environment concepts and therefore make the control environment well-defined. The increased emphasis of COSO on the competence, integrity, and ethics of entity personnel is reflected in amendments to SAS 55 made by SAS 78.

Information and Communication Systems: COBIT, SAC, COSO, and SASs 55/78 differ in their focus and depth of treatment of information systems. COBIT's exclusive focus is the establishment of a reference framework for security and control in information technology. It defines a clear linkage between information systems controls and business objectives. In addition, it provides globally validated control objectives for each information technology process which gives pragmatic control guidance to all interested parties. COBIT also provides a vehicle to facilitate communications among management, users and auditors regarding information systems controls.

SAC focuses on automated information systems. The document examines the interrelationships among internal control and systems software, application systems, and end-user and department systems. Systems software provides the operating system, telecommunications, data management, and other utility functions required by application systems. Application systems include the entity's business, financial, and operational (e.g., human resource, accounts receivable, and production scheduling, respectively) systems. End-user and departmental systems serve the needs of specific groups of users. Many of the volumes of the SAC report provide guidance on internal control needed in each of these areas.

COSO discusses both information and communication. In its discussion of information, COSO reviews the need to capture pertinent internal and external information, the potential of strategic and integrated systems, and the need for data quality. The discussion of communication focuses on conveying internal control matters, and gathering competitive, economic, and legislative information. SAS 55 as amended by SAS 78 is more abbreviated than the other documents; it outlines the objectives of an accounting system and summarizes the COSO material.

Control Activities: COBIT and SAC examine control procedures relative to an entity's automated information system; COSO and SASs 55/78 discuss the control procedures and activities used throughout an entity. COBIT classifies controls into 32 processes naturally grouped into four domains applicable to any information processing environment. SAC uses five different classification schemes for IS control procedures. COSO and SASs 55/78 only use one classification scheme for information system (IS) control procedures. COSO's discussion of control activities stresses who performs the activities and operational rather than financial reporting objectives. COSO also emphasizes the desirability of integrating control

activities with risk assessment. SAS 78 replaces SAS 55's list of control procedures with an abbreviated list of COSO's control activities. In contrast to COSO, SASs 55/78 contain little discussion of these activities. *Risk Assessment:* COSO and SAS 78 identify risk assessment as an important component of internal control. COBIT identifies a process within the information technology environment as assessing risks. This particular process falls into the planning and organization domain and has six specific control objectives associated with it. Although risk assessment is not an explicit component of SAC's system of internal control, the document contains extensive discussions of risk. SASs 55/78 categorize risk into inherent risk, control risk, and detection risk. External auditors understand, test, and assess controls relative to the risk of material misstatements in the financial statements, i.e., relative to the risk of failing to achieve financial reporting objectives. Because they cannot directly alter internal controls, external auditors adjust acceptable detection risk inversely to the assessment of control risk.

COBIT addresses, in depth, several components of risk assessment in an information technology environment. These include business risk assessment, the risk assessment approach, risk identification, risk measurement, risk action plan and risk acceptance. It deals directly with information technology types of risk such as technology, security, continuity and regulatory risks. Additionally, it addresses risk from both a global and system-specific perspective.

The risk concepts presented in SAC and COSO are similar. In addition to the risk of failing to meet financial reporting objectives, SAC and COSO address the risks of failing to meet compliance and, especially, operational objectives. COSO discusses identification of external and internal risks to the entire entity and to individual activities. COSO also considers management's analysis of risk: estimating the significance of a risk, assessing its probability of occurrence, and considering how to manage the risk. SAC examines risks to the automated information system. SAC provides a detailed analysis of IS risks and explores how each of these risks could be mitigated. SAC and COSO emphasize cost/benefit considerations, the need to interrelate entity objectives and controls, the on-going nature of risk identification and assessment, and management's ability to adjust the entity's internal control system.

SASs 55/78 say little about operational or compliance risk. External auditors understand, test, and assess controls relative to the risk of material misstatements in the financial statements, i.e., to the risk of failing to achieve financial reporting objectives. SASs 55/78 categorize risk into inherent risk, detection risk, and control risk. Because they cannot directly alter internal controls, external auditors adjust acceptable detection risk inversely to their assessment of control risk.

Monitoring: In contrast to COBIT, COSO and SASs 55/78, SAC does not explicitly include monitoring as a component of the system of internal control. All the documents assign management the responsibility of ensuring that controls continue to operate properly. COBIT addresses management's responsibility to monitor all information technology processes and the need to obtain independent assurance on controls. It classifies monitoring as a domain -- in line with the management cycle. SAC recognizes internal auditors' responsibilities to select areas of information technology where independent review can yield the greatest benefits and to test controls for evidence of ongoing compliance and effectiveness. Because internal controls should and do evolve over time, COSO recognizes the need for management to monitor the entire internal control system through the ongoing activities built into the control system itself and through special evaluations directed at specific activities or areas.

While SAC and COSO share the same (internal) perspective, COSO discusses monitoring activities in broad terms and SAC discusses specific monitoring activities that should be performed by or within the entity's automated information systems. COBIT in a like, but more in-depth fashion, defines specific monitoring requirements and responsibilities within the information technology function. SAS 55, as amended by SAS 78, presents an abbreviated version of the COSO material that emphasizes the financial reporting objective. Some ongoing monitoring by the external auditor is implied by the assumption that auditors use knowledge obtained through previous audits of the entity.

Reporting Internal Control Problems

As a framework, COBIT provides the definition of controls and the control objectives for specific information technology processes. Similar to COSO, COBIT reports of internal control problems are assumed to be available from a variety of sources to the responsible business process owner. These can range from control self-assessment to external audit reviews -- all conducted using the COBIT framework.

SAC assigns internal auditors the responsibility of evaluating whether appropriate controls are in place and whether these controls are functioning as designed. Internal auditors submit the results of their financial, operational, and information system audits to management and the audit committee. They should articulate the costs and benefits of proposed changes to remedy deficiencies in the system of internal controls. COSO discusses how management collects and disseminates information about internal control deficiencies. Management may learn of deficiencies through reports generated by the internal control system itself, evaluations performed by management or internal auditors, or communications from external parties such as customers, regulators, or external auditors. Management wants information regarding any deficiency that could affect the entity's ability to achieve its operational, financial reporting, or compliance objectives. COSO recommends that entity personnel report deficiencies to immediate supervisors and to management at least one level above the directly responsible person. Separate communication channels should exist for reporting sensitive information.

SASs 55 and 78 focus on the relationship between internal controls and planning an audit of financial statements. SAS 60, Communication of Internal Control Structure Matters Noted in an Audit (as amended by Appendix C of SAS 78), provides guidance to external auditors concerning reporting internal control problems found during a financial statement audit. SAS 60 requires auditors to report significant deficiencies which could affect the entity's financial reporting ability to the audit committee. Auditors may report other problems or improvement opportunities to management.

Period of Time versus Point in Time

COBIT is a model framework. It supports evaluations as either point in time or period of time, depending on the reviewer's preference.

Although SAC does not explicitly state whether internal effectiveness should be evaluated at a point in time or for a period of time, it appears more supportive of period of time evaluations. For example, SAC speaks of ensuring the reliability of financial and operating data, describes using embedded audit modules to continuously monitor and analyze transactions, and recommends employing change controls to ensure the stability of application and systems software.

Although COSO stresses internal control as a process, the report states that internal control effectiveness is a state or condition of the process at a point in time. If internal control deficiencies have been corrected as of the reporting date, COSO approves management reports to external parties that describe internal control as being effective.

SASs 55 and 78 state that external auditors should evaluate the consistency with which controls were applied during the audit period. The Standards caution auditors to supplement tests of controls that only pertain to a point in time with procedures that provide evidence about control effectiveness for the entire audit period.

Tools

COBIT provides explicit guidance for all 32 of the processes it defines. This guidance takes the form of over 250 control objectives. It further provides navigation aids which all users, depending on their particular perspective, implement to organize and categorize control objectives according to IT processes, information criteria or IT resource views of controls.

SAC provides detailed guidance about the controls needed in the development, implementation, and operation of automated information systems throughout most of the 12 modules. In particular, many modules contain sections on the risks and controls associated with the topics discussed in that module. The COSO report provides the reader with tools which may be used to evaluate the system of internal control. An entire volume is devoted to suggested forms for use in examining controls and to samples of completed forms.

While SASs 55/78 themselves do not present forms or tools to use in control evaluation, the companion Audit Guide, Consideration of the Internal Control Structure in a Financial Statement Audit, does. The Guide provides extensive examples of documentation of the understanding of internal control and the assessment of control risk for three companies of varying sizes and characteristics. In addition, the main body of the Guide discusses the evaluation of internal control and the related documentation at length.

Conclusion

Internal and external pressures motivate the accounting and management professions to continue to develop and refine internal control concepts. This article summarizes and compares important documents resulting from these efforts: COBIT, SAC, COSO, and SASs 55 and 78.

COBIT is a globally validated collection of control objectives, organized into processes and domains and linked to business requirements for information. SAC offers detailed guidance about the effects of various aspects of information technology on the system of internal controls. COSO presents a common definition of internal control and emphasizes that internal controls help organizations achieve effective and efficient operations, reliable financial reporting, and compliance with applicable laws and regulations. The document provides guidance on assessing control systems, reporting publicly on internal control, and conducting evaluations of control systems. SAS 55, as amended by SAS 78, adopts COSO's five components of internal control, discusses the effect of the entity's internal control on planning and performing a financial statement audit, and addresses the relationship between internal controls and control risk.

COBIT, COSO, SAC and SASs 55/78 contain many of the same internal control concepts; indeed, later documents build on internal control concepts developed in earlier ones. The documents differ in the audience addressed, the purpose of the document, and level of detail of guidance provided. Although other parties will find each of the documents useful, COBIT is directed to three distinct audiences: management, users and information systems auditors; SAC is primarily addressed to internal auditors; COSO to managers and boards of directors; and SASs 55 and 78 to external auditors.

COBIT is focused exclusively on controls over information technology in support of business objectives. SAC stresses information technology, COSO provides a broad, entity-level view, and SASs 55 and 78 focus on financial statement audits. SAC and COSO are self-contained documents. SASs 55 and 78 are part of a set of standards. The four documents complement and support one another. SAC, COSO, and SASs 55/78 are useful to the primary audiences of the other documents, to legislators, to stakeholders, and to others interested in understanding or improving internal control.

Endnotes

¹ American Institute of Certified Public Accountants (AICPA). 1983. *Audit Risk and Materiality in Conducting an Audit (SAS 47)*.

² American Institute of Certified Public Accountants (AICPA). 1988a. *Communication of Internal Control Structure Related Matters Noted in an Audit (SAS 60)*.

³ American Institute of Certified Public Accountants (AICPA). 1988b. *Consideration of the Internal Control Structure in a Financial Statement Audit (SAS 55)*.

⁴ American Institute of Certified Public Accountants (AICPA). 1990. *Consideration of the Internal Control Structure in a Financial Statement Audit (Audit Guide for SAS 55)*.

⁵ American Institute of Certified Public Accountants (AICPA). 1993. *Reporting on an Entity's Internal Control Structure over Financial Reporting (Statement on Standards for Attestation Engagements 2)*.

⁶ American Institute of Certified Public Accountants (AICPA). 1995. "Consideration of Internal Control in a Financial Statement Audit: An Amendment to SAS No. 55" (SAS 78).

⁷ Committee of Sponsoring Organizations of the Treadway Commission (CSOTC). 1992. *Internal Control - Integrated Framework (COSO Report)*.

⁸ Information Systems Audit and Control Foundation (ISACF). 1995. *COBIT: Control Objectives for Information and related Technology*.

⁹ Institute of Internal Auditors Research Foundation (IIARF). 1991, revised 1994. *Systems Auditability and Control*.

¹⁰ Winters, A.J., and D.M. Guy. 1992. *Internal Control: Progress and Perils*. Proceedings of the 1992 Deloitte & Touche/University of Kansas Symposium on Auditing Problems, pp.177-191.

Janet L. Colbert, Ph.D., CPA, CIA is the Meany-Holland professor of accounting at Western Kentucky University in Bowling Green, KY, USA.

Paul L. Bowen, Ph.D., CPA is a lecturer in the department of commerce at the University of Queensland in Brisbane, Queensland, Australia.