CHAPTER TWO

2 Using CobiT to Perform IT Audits

THE COMMITTEE OF SPONSORING Organizations (COSO) internal controls framework, as introduced and discussed in Chapter 1, has become the standard tool for measuring and evaluating internal accounting controls for a wide span of systems and processes since the 1990s and under the Sarbanes-Oxley Act (SOx). However, some professionals, and information technology (IT) auditors in particular, have expressed concerns about using the COSO internal controls framework in today's IT-oriented world. The concern is that the published COSO internal controls guidance just does not give enough emphasis to IT tools and processes. For example, the published COSO internal controls guidance materials (see Chapter 3) look at IT application internal controls only at a very high level, when there appears to be a need for more IT-specific internal control guidance.

A more IT-oriented internal controls framework, called CobiT (*C*ontrol *Ob*jectives for *I*nformation and related *T*echnology), was in place long before SOx; it was first released in 1996. Although earlier CobiT versions were more oriented to providing IT auditor and controls guidance, CoboT has became a preferred tool for complying with SOx Section 404 internal controls procedures for many enterprises. CobiT provides guidance on evaluating and understanding internal controls, with an emphasis on enterprise IT resources. CobiT is not a replacement for the COSO internal controls framework but is a different way to look at internal controls in today's IT-centric world.

Although originally launched as guidance to help those professionals once called computer auditors—specialist internal and external auditors who reviewed IT-related internal controls—CobiT has evolved into a helpful tool for evaluating all internal controls across an enterprise. CobiT emphasizes the linkage of IT with other business resources to deliver overall values to an enterprise today. This chapter provides an overview of the CobiT framework and its key components. More important, the chapter

describes the relationship between CobiT objectives and the COSO internal control framework for use in all internal audit reviews.

CobiT and its related principles can be used or mapped to other IT initiatives as well. For example, Chapter 11 on software engineering and Capability Maturity Model for integration (CMMi) highlights CMMi linkages to CobiT, as does Chapter 25's discussion on the ISO 17799 standards. In addition, Chapter 16 introduces the related Val IT, an approach to better recognize the value of all IT assets in the enterprise. Val IT addresses assumptions, costs, risks, and outcomes related to a balanced portfolio of IT-enabled business investments.

Even if an internal auditor does not use the CobiT framework in reviews of internal controls, all IT and internal auditors should have a high-level knowledge of the basic CobiT framework. As mentioned, CobiT had its origins as an IT audit guidance tool, but it is much broader today. In addition to the COSO internal controls framework, knowledge of CobiT will help an internal auditor to better understand the role of IT controls and risks in many enterprise environments.

INTRODUCTION TO CobiT

An unusual word for many, CobiT is an acronym that is becoming increasingly recognized by auditors, IT professionals, and many enterprise managers. CobiT is an important internal control framework that can stand by itself but is an important support tool for documenting and understanding COSO and SOx internal controls and recognizing the value of IT assets in an enterprise. A general or working knowledge of CobiT should be an IT auditor requirement.

The CobiT standards and framework are issued and regularly updated by the IT Governance Institute (ITGI) and their closely affiliated professional organization, the Information Systems Audit and Control Association (ISACA). ISACA is more focused on IT auditing while ITGI's emphasis is on research and governance processes. ISACA also manages the Certified Information Systems Auditor (CISA) examination and professional designation as well as its newer Certified Information Systems Manager (CISM) and the Certified in the Governance of Enterprise IT (CGEIT) certification and examination. The Certified Information Security Manager (CISM) certification targets IT security managers and promotes the advancement of professionals who wish to be recognized for their IT governance-related experience and knowledge. These audit-related professional certifications are discussed in Chapter 30. ISACA was originally known as the EDP Auditor's Association (EDPAA), a professional group begun in 1967 by internal auditors who felt that their then current professional organization, the Institute of Internal Auditors (IIA), was not giving sufficient attention to the importance of IT systems and technology controls as part of internal audit activities. We have almost forgotten that EDP once stood for electronic data processing, today an almost archaic term for IT. Over time, this professional enterprise broadened its focus and became ISACA, while the IIA has also long since embraced strong technology issues.

The EDPAA, originally an upstart IT audit professional organization, began to develop IT audit professional guidance materials shortly after its formation. Just as the

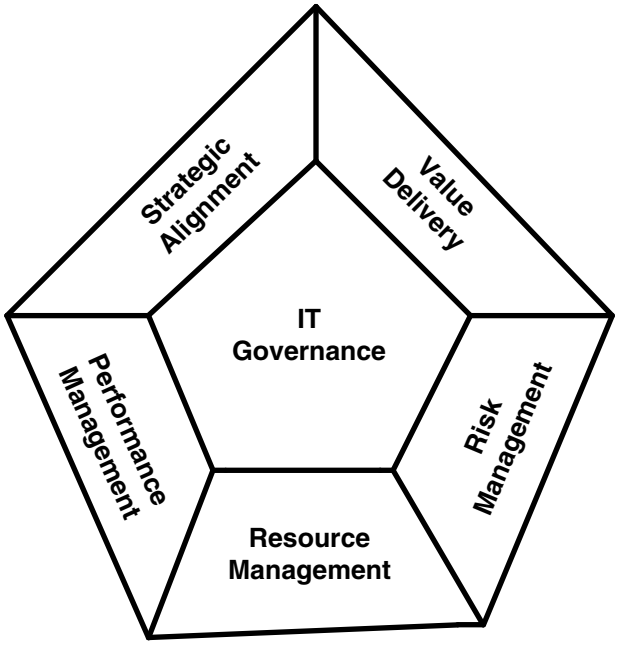

EXHIBIT 2.1 CobiT IT Governance Focus Areas

EDPAA evolved into the well-respected ISACA and now the ITGI, its original IT audit standards became an excellent set of internal control objectives that evolved to CobiT, now in its 2007 version 4.1 edition.[1] With virtually all enterprise processes today tied to IT-related facilities, an understanding of the overall area of IT governance is critical. The CobiT framework is often described as a pentagon covering five broad and interconnected areas of internal controls, as illustrated in Exhibit 2.1. The exhibit shows CobiT's major areas of emphasis arranged around the important core concept of IT governance:

1. **Strategic alignment.** Efforts should be in place to align IT operations and activities with all other enterprise operations. These efforts include establishing linkages between enterprise business operations and IT plans as well as processes for defining, maintaining, and validating quality and value relationships.
2. **Value delivery.** Processes should be in place to ensure that IT and other operating units deliver promised benefits throughout a delivery cycle and with a strategy that optimizes costs while emphasizing the intrinsic values of IT and related activities.
3. **Risk management.** Management, at all levels, should have a clear understanding of an enterprise's appetite for risk, compliance requirements, and the impact of significant risks. Both IT and other operations have their own and joint risk management responsibilities that may individually or jointly impact the entire enterprise.
4. **Resource management.** With an emphasis on IT, there should be an optimal investment in, and the proper management of, critical IT resources, applications,

information, infrastructure, and people. Effective IT governance depends on the optimization of knowledge and infrastructure.

5. **Performance measurement.** Processes should be in place to track and monitor strategy implementation, project completions, resource usage, process performance, and service delivery. IT governance mechanisms should translate implementation strategies into actions and measurements to achieve these goals.

These five CobiT internal control concerns are the elements of the CobiT framework and define IT governance. The CobiT framework is an effective tool for documenting IT and all other internal controls. This chapter looks this framework in the broader perspective of using CobiT to assist in the IT governance processes of management, enterprise, and internal auditing.

The following sections provide an overall description of the CobiT framework and its key elements to link business with IT goals through key controls and effective measurement metrics. In addition, the chapter describes mapping CobiT standards with the COSO internal control framework, discussed in Chapter 1, with the information technology infrastructure library (ITIL) best practices introduced in Chapter 7, and for overall IT and corporate governance. Elements and key components of IT governance are discussed as well. The CobiT framework is an effective mechanism for documenting and understanding internal controls at all levels. Although CobiT first started primarily as a set of ''IT audit'' guidance materials, it is a much more powerful tool today.

CobiT FRAMEWORK

IT processes and their supporting software applications and hardware devices are key components in any enterprise today. Whether a small retail business with a need to keep track of its inventory and pay employees, or a large Fortune 50 corporation, all need a wide set of interconnected and often complex IT processes that are closely tied to their business operations. That is, enterprise business processes and their supporting IT resources should work in a close information-sharing relationship. IT cannot and certainly should not tell business operations what types of IT processes and systems to implement, but IT provides information to help influence business decisions. In the very early days of computer systems, often IT managers felt they had lots of answers and promoted systems solutions to their businesses, sometimes with very counterproductive results. However, this relationship has changed today; IT and business operations generally should have a close mutual relationship of shared requirements and information. Internal auditors must understand the needs and information-sharing requirements on both sides. As discussed in Chapter 1 in the COSO internal controls framework, IT has responsibilities over a series of other related process areas that are audited by or through established audit guidelines, are measured by a series of performance indicator measures and activities, and are made effective through activity goals. All of these can also easily become part of CobiT, a control framework including both IT and business processes.

Chapter 1 described the COSO internal control framework and its importance in defining SOx internal controls. An IT auditor might ask, ''I understand and use COSO

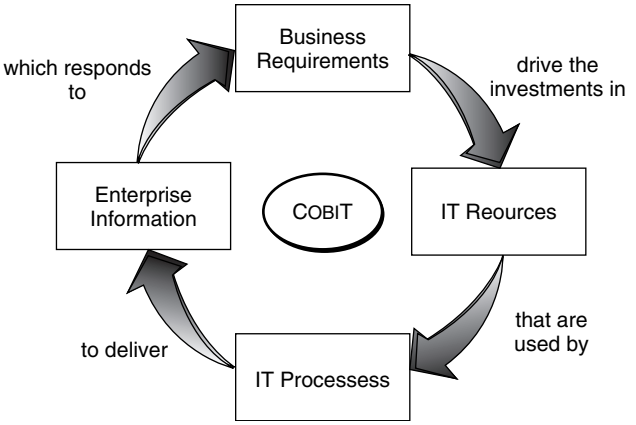

EXHIBIT 2.2 Basic CobiT Principles
Source: COBIT 4.1 © 1996–2001 IT Governance Institute. All rights reserved. Used by permission.

internal controls. Why another framework?'' The answer here is that CobiT provides *an alternative* approach to define and describe internal controls that has more of an IT emphasis than the pure COSO internal controls framework. Information and supporting IT processes often are the most valuable assets for all enterprises today, and management has a major responsibility to safeguard its supporting IT assets, including their automated systems. Management, users, and IT auditors all need to understand these information-related processes and the controls that support them. This combination of IT processes amd internal controls focuses on the effectiveness and efficiency of IT resources, processes, and overall business requirements. Exhibit 2.2 describes these basic CobiT principles, with business requirements driving the demand for IT resources and those resources initiating IT processes and enterprise information in a continuous, circular manner. Management should be interested in the quality, cost, and appropriate delivery of its IT-related resources whose control components are the same as the COSO internal control elements discussed in Chapter 1. Internal controls over IT resources are very much based on the effectiveness and efficiency interdependencies of these IT components.

IT governance is a key concept that was not strongly emphasized as a CobiT element prior to SOx. It is an important internal control concept today with the ITGI playing a strong leadership role. As described in the IT governance pentagon in Exhibit 2.1, CobiT defines IT governance as a series of key areas ranging from keeping focus on strategic alignments to the importance of both risk and performance measurement when managing IT resources. We refer to this IT governance pentagon again as we navigate through the CobiT framework.

CobiT looks at internal controls from three IT dimensions: resources, processes, and information criteria, described in the CobiT Cube illustrated in Exhibit 2.3. Similar to the COSO internal controls framework cube discussed in Chapter 1 and Chapter 4 on the COSO ERM framework, this CobiT model looks at IT controls from a three-dimensional perspective. That is, each component on one surface relates to the two other connecting dimensions. However, CobiT's front-facing dimension with its pictorial descriptions of

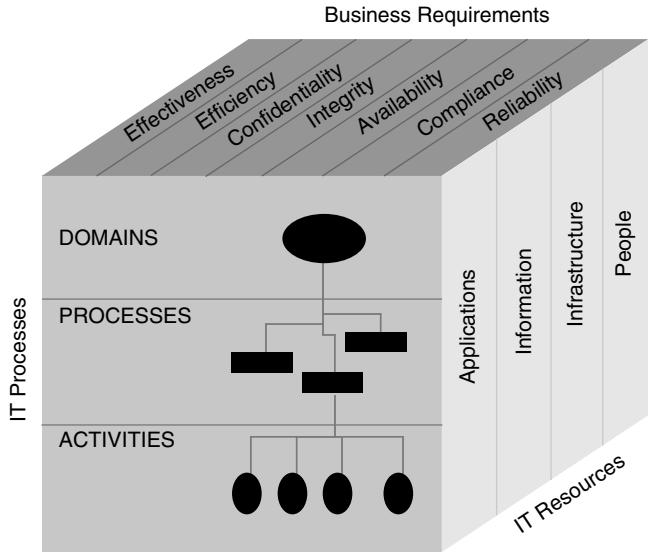

EXHIBIT 2.3 CobiT Cube
Source: COBIT 4.1 ©1996–2001 IT Governance Institute. All rights reserved. Used by permission.

process flow diagrams sometimes scared off non-IT people from considering CobiT. The non–IT savvy professional—and there are many—may look at the process diagrams on the face of the CobiT cube and decide this approach must be too technical. This is not at all correct. We describe and explain the CobiT framework and why it can be valuable for understanding SOx internal controls and improving both IT audit and governance practices in the next sections.

CobiT Cube Components

IT Resources

The IT resources side of the three-dimensional CobiT cube framework represents all of an enterprise's IT assets, including its people, the application systems, installed technology, IT facilities, and the value of data. The right-hand side of the framework cube represents the necessary concerns and considerations for all of the resources necessary for the control and administration of enterprise IT resources. Either individually or as groups, these resources should be considered when evaluating controls in an IT environment:

- Applications consisting of both automated user systems and manual or automated procedures to process information
- Information, including input, output, and processed data, for use by business processes
- Technology and facility infrastructure components including hardware, operating systems, databases, networks, and the environments that house and support them
- Key and specialized personnel to plan, organize, acquire, implement, support, monitor, and evaluate IT services

We have started our CobiT description from the right-hand side of the CobiT cube, but internal control considerations always must be considered in terms of how they relate to other components on that side of the CobiT cube as well as with others in this three-dimensional perspective. The point here is that IT resources should always be considered as a key component to IT governance and internal controls.

IT Processes

The second and front-facing dimension of the CobiT cube refers to IT processes and consists of three segments: domains, processes, and activities. Domains are groupings of IT activities that match to organizational areas of responsibility, with four specific domain areas defined in CobiT:

1. **Planning and enterprise.** This domain area covers the strategy and tactics that allow IT to best contribute to and support enterprise business objectives. This type of IT strategic vision message should be communicated throughout the enterprise—the message of IT's mission and what it is trying to accomplish for the overall enterprise.
2. **Acquisition and implementation.** IT solutions need to be identified, developed, or acquired and both implemented and integrated with business processes. This domain area covers changes and maintenance of existing systems.
3. **Delivery and support.** This domain area covers the actual delivery of required services, both application and infrastructure tools. The actual process of application data and controls is covered within this domain.
4. **Monitoring and evaluation.** This area includes control processes, including quality and compliance monitoring, as well as external and internal audit evaluation procedures.

Within an IT enterprise, the process to identify and build new applications—traditionally called systems development life cycle (SDLC) procedures—could be viewed as part of the CobiT implementation domain, and quality assurance could be viewed as part of the monitoring domain. For the planning and enterprise domain, CobiT suggests these specific processes:

- Define a strategic IT plan.
- Define the information architecture.
- Determine technological direction.
- Define the IT enterprise and relationships.
- Manage the IT investment.
- Communicate management aims and direction.
- Manage human resources.
- Ensure compliance with external requirements.
- Assess risks.
- Manage projects.
- Manage quality.

Individual processes are the next level down. They are a series of joined activities with natural control breaks. Finally, activities are the actions needed to achieve measurable results. Activities have a life cycle whereas tasks are discrete. We can think of the systems development life cycle (SDLC) process as a cycle where a new application is designed, implemented, operated over time, and then replaced with an improved process.

Business Requirements

The third dimension of the CobiT model consists of business requirements. These seven components should be considered when evaluating all business requirements and with consideration given to the following necessary IT resources and process criteria elements:

1. Effectiveness
2. Efficiency
3. Confidentiality
4. Integrity
5. Availability
6. Compliance
7. Reliability

All IT overall systems or processes should be evaluated with consideration given to one or more of these seven criteria areas. Emphasis will vary, but all IT processes should have elements of one or more of these criteria. For example, for a given IT application, an IT auditor may be concerned about its confidentiality and integrity controls. Business functions typically establish such requirements for their general business needs. For IT applications, each of these attributes is discussed in more detail in the next section as well as in Chapter 8 on planning and performing IT general controls audits.

Similar to the COSO cube internal control model from Chapter 1 and the COSO enterprise risk framework discussed in Chapter 4, the CobiT cube presents an effective way to understand the relationships among business requirements, IT processes, and IT resources. The three-dimensional nature of the model emphasizes the cross relationships and interdependencies between business and IT processes. In our IT-dependent world, this is a useful way for an IT auditor to look at and understand internal controls. CobiT is a rich—sometimes almost too rich—set of processes for focusing on business and IT goals and key controls, and for identifying key measurement metrics. The next sections discuss CobiT in some detail, but the reader is encouraged to consult the ITGI's CobiT reference materials at www.isaca.org for further information.

USING CobiT TO ASSESS INTERNAL CONTROLS

Besides the CobiT cube, with its forward face showing process flow diagrams to emphasize relationships, the published CobiT guidance materials[2] can look formidable to many internal auditors and other business professionals as well as even some IT professionals. The basic CobiT reference material is published in a nearly 200-page manual filled with an array of charts and tables. It is a useful set of materials, but some study may be

required to fully understand the concepts behind the CobiT framework. The following sections should help an IT auditor to navigate through the published CobiT framework, and more importantly, use it to develop and assess enterprise internal controls.

Although any dimension of the CobiT cube can be used to understand control environments, the four previously discussed domains, starting with Planning and Enterprise, is an effective first step in the CobiT cube diagram. Based on these initial three CobiT control cube dimensions, each IT process should be evaluated through these five navigation steps:

I. The control of [*Process Name*]
II. Which satisfy [*List of Business Requirements*]
III. By focusing on [*List of important IT goals*]
IV. Is achieved by [*List of Control Statements*]
V. And is measured by [*List of key metrics*]

This five-step process dialogue can go from number I on down or can start at the base level and navigate up. In either case, the CobiT framework says that the control of any process should be satisfied by a list of supporting business requirements and that those business goals should focus on important IT goals. This only makes sense. A designated process would just be an idle name unless supported by specific business and IT requirements to drive and govern that process. Each of those requirements should be defined by one or more control statements with specific control practices. Finally, we must assess whether matters are operating effectively, and key measurement metrics are necessary. Although CobiT's emphasis historically has been on IT, this type of analysis should be used for a wide range of internal control–related audits, IT related or not.

Each major control objective described in the published CobiT guidance material is based on the ITGI's navigation framework shown in Exhibit 2.4. The upper left corner of that exhibit shows business requirements. While this is a blank sample, in the published CobiT guidance, each of these requirements are marked with a P to indicate a primary requirement, S for a secondary, or left blank for a not applicable control objective. The lower right-hand corner lists the IT resource areas. If any are applicable, they are noted with a check mark. The lower left-hand corner shows the same pentagon diagram we saw in Exhibit 2.1. Here sections are shaded or marked if they are of primary or secondary importance.

The center of each of the CobiT guidance pages has the ''Control over the IT Process of . . . '' series of statements completed for each control objective. We will show examples of completed statements as we review the CobiT domains. Even though the CobiT navigation and supporting documentation is thorough and somewhat elegant, it can scare away first-time some auditors. The next sections look at CobiT navigation across various selected domains to give a feel for its organization. Even if auditors are accustomed to using the COSO internal controls framework, they should at least experiment with using CobiT in selected reviews. This chapter provides an introduction and overview to CobiT, its supporting ITGI professional organization has a wide variety of published and educational offerings on the use of CobiT that can be found on previously referenced Web site www.isaca.org.

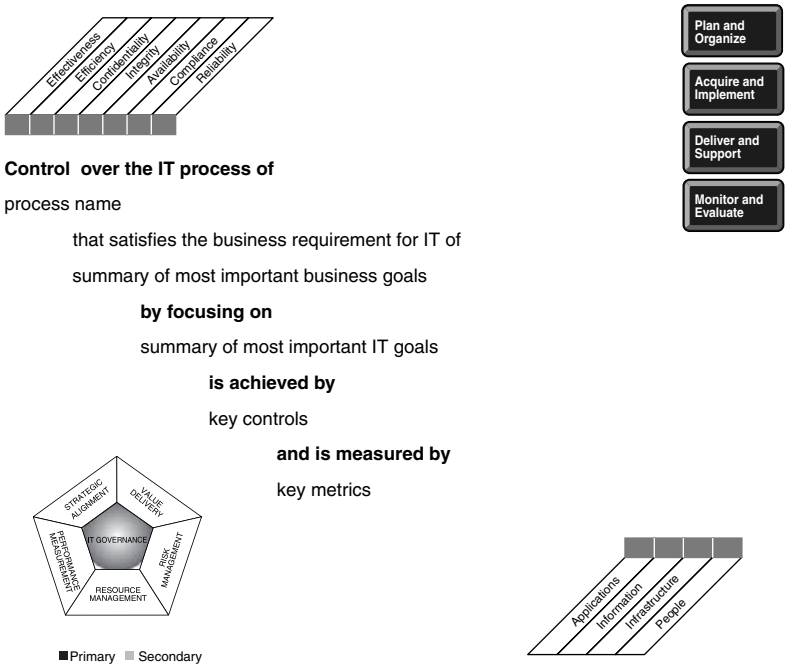

EXHIBIT 2.4 Navigating the CobiT Framework
Source: COBIT 4.1 ©1996–2001 IT Governance Institute. All rights reserved. Used by permission.

Planning and Enterprise

CobiT calls for a high level group of processes that set the direction for the enterprise and its IT resources. For this domain, CobiT has 10 high-level Planning and Organizing (PO) control objectives, defined and numbered as follows:

PO1	Define a Strategic Plan
PO2	Define the Information Architecture
PO3	Determine Technological Direction
PO4	Define IT Process, Enterprise, and Relationships
PO5	Manage the IT Investment
PO6	Communicate Management Aims and Direction
PO7	Manage IT Human Resources
PO8	Manage Quality
PO9	Assess and Manage IT Risks
PO10	Manage Projects

These are all very high-level concepts. Many IT professionals and other managers might say "Of course!" when an internal auditor asks whether they have such a strategic plan, have defined their information architecture, or are in compliance with any of the other high-level PO objectives. However, CobiT drills down into its defined control objective areas in greater detail. While many of the issues are similar, this is in strong contrast to the monitoring element of COSO internal controls as discussed in

Chapter 1. There, the concepts are only at a fairly high level; CobiT is much more specific. For example, using the PO1 control objective on defining a strategic plan, CobiT then expands this to six more detailed objectives:

PO1.1 IT Value Management
PO1.2 Business-IT Alignment
PO1.3 Assessment of Current Performance
PO1.4 IT Strategic Plans
PO1.5 IT Tactical Plans
PO1.6 IT Portfolio Management

The numbering here is important as the published CobiT guidance materials references each of these and other objectives in terms of references to their inputs and outputs. CobiT's published materials provides a high-level description for each of these objectives. For example, the PO1.4 objective on strategic plans states:

> Create a strategic plan that defines, in co-operation with the relevant stakeholders, how IT will contribute to the enterprise's strategic objectives (goals) and related costs and risks. It includes how IT will support IT-enabled investment programs and operational service delivery. It defines how the objectives will be met and measures and will receive formal sign-off from the stakeholders. The IT strategic plan should cover investment/operational budget, funding sources, sourcing strategy, acquisition strategy, and legal and regulatory requirements. The strategic plan should be sufficiently detailed to allow the definition of tactical IT plans.

This paragraph is an example of one of the many control objectives outlined throughout the CobiT guidance. All are covered elsewhere. The objectives here do not tell the professional *how* to write an IT strategic plan but do provide excellent guidance to build such a plan, no matter the size or status of the enterprise. These general objectives are also good tools for internal auditors in their needs to build review criteria in any of these areas. IT auditors can develop those audit objectives by taking each sentence of the objectives and developing audit review areas.

For each of the CobiT objectives, the guidance material also contains what is called a supporting RACI chart. A tool that evolved from quality initiatives in the 1960s, RACI charts are good tools to identify roles and responsibilities. Using a spreadsheet format, activities are identified in a side column and functions or position descriptions are located in cells across the top. Responsibilities for those activities are identified in intersecting cells through one or several of the RACI initials:

R = **Responsible** (who owns the problem or process)
A = **Accountable** (who must sign off on the activity before it is effective)
C = **Consulted** (who has the information and/or capability to complete the work)
I = **Informed** (who must be informed of the results but need not be consulted)

This type of chart can be useful in many areas to help identify responsibilities over multiple areas. Exhibit 2.5 is a RACI chart, adapted from CobiT materials, on the PO1 objective to define a strategic IT plan. Going down the column of responsibilities, in this

CobiT PO1 Activities	CEO	CFO	Business Executive	CIO	Process Owner	Head of Operations	Head IT Admin.	Internal Audit
Link Business Goals to IT Goals	C	I	A/R	R	C			
Identify Critical Dependencies and Current Performance	C	C	R	A/R	C	C	C	C
Build an IT Strategic Plan	A	C	C	R	I	C	C	C
Build IT Tactical Plans	C	I		A	C	C	C	I
Analyze Program Portfolios and Manage Service Portfolios	C	I	I	A	R	C	C	I

EXHIBIT 2.5 RACI Chart Example

example, the Business Process Owner acts as a **C**onsultant on linking business goals, building tactical plans, and identifying critical dependencies; is **I**nformed on processes for building the strategic plan; and is **R**esponsible for analyzing program portfolios. The chart outlines responsibilities for such people as the enterprise's head of IT or chief information officer (CIO), the process owner, and internal audit. This type of RACI chart appears in the published guidance for each of the CobiT control objectives.

The CobiT material concludes with a summary analysis of the control objective. This is a metrics-based set of considerations that outlines the activity goals for a given control objective that are measured by key performance indicators (KPIs) that drive process goals and are measured by process-related key goal indicators. The latter drive IT goals that are measured by IT key goal indicators. This CobiT documentation is explained in more detail as we review the other CobiT control objectives.

For the major control objective, the guidance material discusses each PO control objective in the same manner and following the same approach with suggested high-level controls review approaches. However, many of these CobiT items may be found only in larger IT enterprises, although the CobiT guidance material has a range of approaches for each objective. For example, the CobiT objective PO3.5 calls for the need for an enterprise IT architecture board or function. This is valuable guidance, but many smaller IT functions do not have the resources to establish such a formal IT architecture board function. Managers who use CobiT and auditors who evaluate compliance should always remember that CobiT is a set of best practices *guidance* materials, not mandatory requirements. Internal auditors should always use the CobiT guidance with some level of caution, recognizing that CobiT often only specifies some very high-level ideal environments. An auditor reviewing IT general controls in a smaller enterprise who follows CobiT guidance to the letter and recommends such a formal "IT Architecture" board could get laughed out of someone's office.

Acquisition and Implementation

Each of the CobiT high-level control objectives discusses the control procedures in the same general format. Whether it is in-house software development efforts or purchased

IT components, the recommended high-level CobiT acquisition and implementation (AI) objectives are:

AI1 Identify Automated Solutions
AI2 Acquire and Maintain Application Software
AI3 Acquire and Maintain Technology Infrastructure
AI4 Enable Operation and Use
AI5 Procure IT Resources
AI6 Manage Changes
AI7 Install and Accredit Solutions and Changes

Each of the detailed objectives in this domain covers control procedures over the implementation of new tools. Although the emphasis is on IT software, the internal control concepts also can be applied to the acquisition and implementation of many new enterprise tools.

Space does not allow complete coverage of each control objective, but we will examine AI6 on managing change as an example of how CobiT uses its basic framework to outline the importance of this control area. For example, earlier we outlined CobiT's five-step process for evaluating control objectives. The outline for these steps appears in the center of the Exhibit 2.4 navigation page. The AI6 objectives on managing changes follow the same five-step process and are outlined in this way:

I. Control over the IT Process of managing changes
   II. That satisfies the business requirement for IT of responding to business requirements in alignment with business strategy, while reducing solution and delivery defects and rework
      III. By focusing on controlling impact assessment, authorization, and implementation of all changes to the IT infrastructure, applications, and technical solutions, minimizing errors due to incomplete request specifications and halting implementation of unauthorized changes
         IV. Is achieved by
            - Defining and communicating change procedures, including emergency changes
            - Assessing, prioritizing, and authorizing changes
            - Tracking status and reporting on changes
         V. And is measured by
            - Number of disruptions or data errors caused by inaccurate specifications or incomplete impact assessment
            - Application or infrastructure rework caused by inadequate change specifications
            - Percent of changes that follow internal change controls processes.

This series of statements, taken from the CobiT guidance materials, describes the control requirements and measure for this AI6 control objective. The CobiT guidance materials have a similar set of statements for each control objective. This summary of

control considerations is useful when attempting to better understand the characteristics of each control.

That same guidance material looks at how each control objective relates to the other two sides of the CobiT cube. For the AI6 managing changes control objective, it indicates that on the IT Resources side, all CobiT defined internal controls are important or have a check mark to help in in understanding this control objective. That is, the control object impacts applications, information, infrastructure, and people. Turning to the upper left side of the navigation sheet business requirements dimension, the guidance material indicates objectives of whether they are of primary, secondary, or of no significant importance. For this AI6 example control objective, the business requirements of effectiveness, efficiency, integrity, and availability are of primary importance while reliability is of secondary importance. The remaining two business requirements, confidentiality and compliance, however are not considered significant to this control objective.

For each control objective, the CobiT guidance material is based on an image of the Exhibit 2.1 focus areas pentagon for the AI6 control objective, and value delivery is of prime importance with resource management secondary. The CobiT guidance material does not provide detailed discussion of the reasons for that designation. Professionals working with the CobiT control objectives usually can deduce why a given IT governance area has been designated as of primary or secondary significance.

Delivery and Support

Following the same general format, the third high-level CobiT control objective is called Delivery and Support (DS). This control objective largely covers service management issues related to the ITIL business process objectives, as discussed in Chapter 7, and highlights some of the changes to our understandings of internal controls that have evolved since the enactment of SOx in 2002. Both CobiT and ITIL were in existence at that time, but the SOx Section 404 emphasis on effective internal controls has brought things together. The CobiT DS control objectives are also similar to the ITIL internal controls to enhance business processes. Both cover the important area of what is known as IT service management, the processes required to ensure efficient IT operations and to deliver these services.

In earlier days, concerns about IT internal controls focused on individual application-by-application controls. Much attention was paid to the higher-level general controls, such as perimeter security or disaster recovery planning, but financial auditors often focused on computational and balancing controls in specific applications. However, no matter how well designed, all such IT applications must operate in an efficient and almost automated process. There will always be smaller problems, such as a legitimate systems user becoming locked out by entering incorrect passwords, and there is a need for efficient service and problem management processes to report and resolve such matters. The CobiT DS control objectives cover many of these important areas:

DS1	Define and Manage Service Levels
DS2	Manage Third-Party Services

DS3 Manage Performance and Capacity
DS4 Ensure Continuous Service
DS5 Ensure Systems Security
DS6 Identify and Allocate Costs
DS7 Educate and Train Users
DS8 Manage Service Desk and Incidents
DS9 Manage the Configuration
DS10 Manage Problems
DS11 Manage Data
DS12 Manage the Physical Environment
DS13 Manage Operations

These control objectives represent important areas of IT operations that historically have not received sufficient attention from IT auditors. The CobiT material looks at each of these objectives in the same general format, summarizing how each control objective is achieved and measured as well as the relationships and interdependencies across all three sides of the CobiT cube.

Many of these control objective areas did not receive sufficient attention in internal controls reviews prior to SOx Section 404 and its Auditing Standard No. 5 (AS 5) rules. COSO objectives address internal controls at a high level but sometimes does not address more detailed service management–related internal control issues. The CobiT DS10 control objective for problem management is an example:

> Effective problem management requires the identification and classification of problems, root cause analysis and resolution of problems. The problem management process also includes identification of recommendations for improvement, maintenance of problem records and review of the status of corrective actions. An effective problem management process improves service levels, reduces costs, and improves customer convenience and satisfaction.

IT users have had problems over the years in reporting problems and seeking resolutions with various systems and applications. Insensitive IT operations staffs frequently did not do an appropriate job in resolving reported problems efficiently. All too often, if an application totally failed, there would be a strong effort to get it back in operation; smaller, less critical problems would be brushed off in a cavalier manner as something to be "considered in the next update."

The published CobiT guidance material links this control objective to others that provide for its inputs as well as outputs. For example, the objectives of AI6 on change authorization, DS8 for incident reporting, DS9 for IT configuration management, and DS13 on error logs all provide inputs to the DS10 control objective. Our purpose is to not reproduce the full contents of all of the published CobiT control objectives but to give the IT auditor a feel for CobiT's approach. Here and for all of the domains and objectives, CobiT provides a powerful way to look at the breadth and depth of these IT-related internal controls and their relationships.

We have discussed how each CobiT control has a series of detailed objectives, has other control inputs and outputs, and has a RACI chart balancing functions and

Activity Goals and Metrics

Assigning sufficient authority to problem manager

Performing root cause analysis of reported problems

Analyzing terms

Taking ownership of problems and problem resolution

are measured by **Key Performance Indicators**

Average duration between the logging of a problem and identification of root cause.

% of problems for which root cause analysis was undertaken

The frequency of reports or updates to an ongoing problem based on its severity.

drive **Process Goals**

Record and track operational problems through resolutions.

Investigate the root cause of all significant problems.

Define solutions for identified operations problems.

are measured by **Process Key Goal Indicators**

% of problems recorded and tracked

% of problems that recur by time and severity

% of problems resolved with required time period

# of open, new, and closed problems by severity

Average and standard deviation of time lag between problem identification and resolution

Average and standard deviation of time lag between problem resolution and closure

drive **IT Goals**

Ensure satisfaction of end users with service offerings and service levels.

Reduce solution and service delivery defects and rework.

Protect the achievement of IT objectives.

are measured by **IT Key Goal Indicators**

# of recurring problems with impact on business

# of business disruptions caused by operational problems

EXHIBIT 2.6 CobiT Example: DS10 Manage Problems Goals and Metrics

responsibilities for each control. In addition, the published CobiT guidance materials have a goals and metrics section for each control objective. Exhibit 2.6 shows this goals and metrics chart for the DS10 Manage Problems control objective. Each published CobiT control objective has a similar set of these very useful analyses. With problem management, for example, three suggested measurement metrics should be

considered. One is performing root cause analyses of reported problems, which is an important goal that is sometimes missed. The related RACI chart highlights that the problem manager is responsible for this activity with others given a consulting role.

Under each activity goal, a table of KPIs follows that drive a set of process goals. With different specific content for each CobiT control, this type of analysis provides all parties with a good set of standards for measuring the performance of control areas and establishing metrics to assess achievement of these goals. This analysis for our selected control objective of problem management is a good example of the power of the published CobiT materials. Many IT operations have some types of help desk function to report and resolve problems. Here, CobiT provides some good suggestions for the types of measures and metrics that can be used to evaluate the achievement of this control objective.

Similar tables of goals and objectives as well as detailed control objectives exist for each CobiT control objective. These are requirements similar to the SOx Section 404 auditing procedures discussed in Chapter 1 or the internal audit professional practice standards referenced in Chapter 3. However, this set of CobiT materials provides excellent guidance materials for establishing and then measuring effective internal controls. IT auditors should become familiar with CobiT,

Monitoring and Evaluation

The fourth CobiT domain is called Monitoring and Evaluation (ME). This set of control objectives emphasizes CobiT as a closed loop process that effectively never ends. CobiT calls for establishing baseline measures to allow an enterprise to measure how it is performing and to provide the enterprise with future opportunities. This domain area covers quality assurance areas that are traditionally more common to manufacturing and other operations areas than they have been to IT. Although not discussed in the CobiT guidance materials, the pioneering quality assurance work of Edward Deming provides a way of considering this CobiT domain area.

A consultant helping to rebuild Japan in the aftermath of World War II, Deming developed quality standards and approaches that helped Japan rebuild and establish the quality practices that are used worldwide today. Among his approaches, Deming developed a quality system that called for business processes to be analyzed and measured to identify the sources of variations that cause products to deviate from customer requirements. He proposed that business processes be viewed or defined in a continuous feedback loop so that managers could identify and change any parts of the process that needed improvement. This concept defines a continuous, never-ending cycle where we should always monitor current process performance and take actions to implement improvements to that process. Deming called this the Plan, Do, Check Act cycle (PDCA), as shown in Exhibit 2.7. The steps here are:

Step 1. Plan. Business processes should be designed or revised to improve results.
Step 2. Do. Implement to plan and measure its performance.
Step 3. Check. Assess the measurements and report the results.
Step 4. Act. Decide on needed changes to improve results.

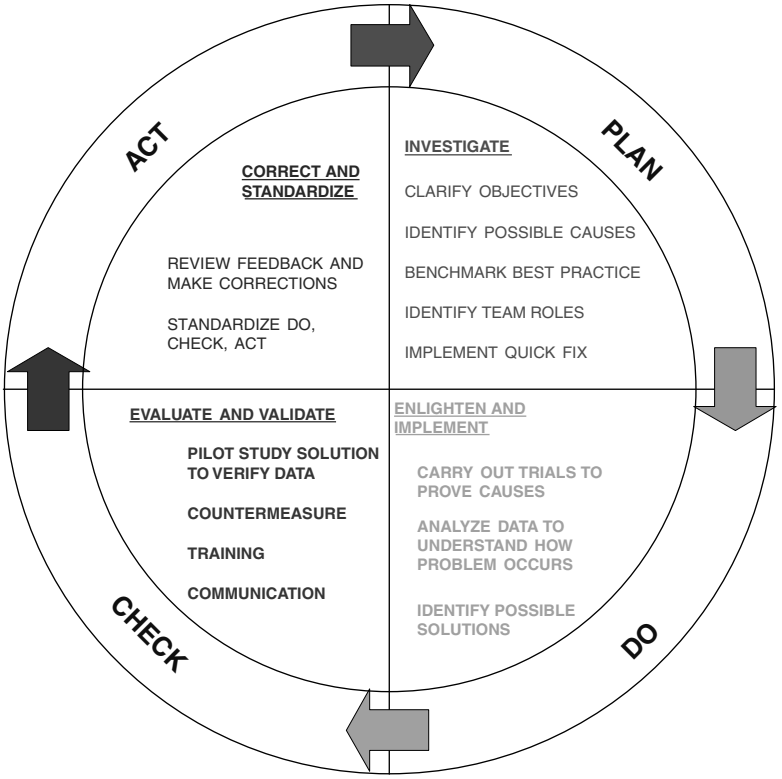

EXHIBIT 2.7 Deming's PDCA Cycle

Source: Robert R. Moeller, *Sarbanes-Oxley Internal Controls: Effective Auditing with AS5, CobiT, and ITIL* (Hoboken, NJ: John Wiley & Sons, 2008). Copyright © 2008 John Wiley & Sons. Reprinted with permission of John Wiley & Sons, Inc.

Although Deming's focus was on postwar reconstruction and on industrial production, his concepts have been carried forward and are very appropriate for today's business environments, including IT operations and SOx internal control monitoring. Chapter 1 discussed the status of SOx today and its continuing monitoring requirements. This CobiT monitoring and evaluation component calls for such continuous monitoring processes.

Following the same format as the other CobiT domains, the ME domain component has four principal control objectives:

ME1	Monitor and Evaluate IT Performance
ME2	Monitor and Evaluate Internal Controls
ME3	Ensure Regulatory Compliance
ME4	Provide IT Governance

This area is of particular interest to internal auditors as well as other members of an enterprise. The control material for ME2 on monitoring and evaluating internal

controls is a good example of CobiT's strength. It states that the process of monitoring and evaluating internal control is achieved by defining the system of IT controls embedded in the IT process framework, by monitoring and reporting on the effectiveness of these internal controls, and by reporting exceptions to management for corrective action. This is really the Deming PDCA process just discussed, and it should be measured by:

- Number of internal control breaches
- Number of control improvement initiatives
- Number and coverage of control self-assessments

As with most of the CobiT framework, the material here focuses on IT controls, but many of these concepts can be generalized to an overall internal controls review process. The term *control self-assessments* refers to the process of ongoing internal reviews on the completeness and effectiveness of internal controls.

This CobiT controls objective has seven detailed supporting objectives. These detailed controls have been somewhat abbreviated from the CobiT guidance materials to describe their essence. Although CobiT is oriented to internal reviews of these primarily IT resource areas, this guidance is particularly important for internal auditors in their reviews of IT and all other internal controls:

ME2.1. Monitoring of the Internal Control Framework. IT auditors should continuously monitor the control environment and framework using industry best practices and benchmarking to improve the control environment and framework.

ME2.2. Supervisory Review. In addition to auditor reviews, CobiT calls for management to monitor and report on the effectiveness of IT internal controls through supervisory reviews, including compliance with policies and standards, information security, change controls, and controls established in service-level agreements.

ME2.3. Control Exceptions. Record information regarding all control exceptions and ensure that it leads to analysis of the underlying cause and to corrective action. Management should decide which exceptions should be communicated to the individual responsible for the function and which exceptions should be escalated.

ME2.4. Control Self-Assessments. IT management should evaluate the completeness and effectiveness of the internal controls over IT processes, policies, and contracts through a continuing program of self-assessment.

ME2.5. Assurance of Internal Control. IT operations should obtain, as needed, further assurance of the completeness and effectiveness of internal controls through third-party reviews by the corporate compliance function, internal audit, outside consultants, or certification bodies.

ME2.6. Internal Control at Third Parties. Assess the status of each internal external provider's internal controls and confirm they comply with legal and regulatory requirements and contractual obligations.

ME2.7. Remedial Actions. Identify and initiate remedial actions based on the controls assessments and reporting. This includes follow-up of all assessments

including: (1) review, negotiation, and establishment of management responses; (2) assignment of responsibility for remediation or risk acceptance; and (3) tracking the results of the actions taken.

These CobiT control objectives are described as ''detailed'' but provide openings for a wide range of even more detailed control procedures. For example, ME2.1 on Monitoring the Internal Control Framework requires IT auditors or other internal controls specialists to develop detailed control procedures that typically may result in a program of many more tests or steps.

This CobiT control objective, as well as all of the others in the supporting documentation, has a section on assessing the maturity of each internal control. *Maturity* here refers to the Capability Maturity Model for Integration (CMMI), introduced in Chapter 11, and a five-level assessment measure designed and developed by Carnegie Mellon University.[3] The model has defined levels for when controls can be assessed from a CMMI level 1 of nonexistent, level 2 as initial or ad hoc controls all the way to level 5, called optimized controls. CobiT rates each of its controls against this CMMI measure. For example, CobiT defines that an enterprise will be at level 3, defined process controls for ME2, Monitor and Evaluate Internal Controls, when management supports and has institutionalized internal control monitoring. The guidance goes on to say that policies and procedures should have been developed for processing and reporting internal control monitoring activities. To achieve this CMMI level, an educational and monitoring program for internal control evaluations should have been defined. CMMI is discussed in greater detail in Chapter 11.

We have shown this limited extract for ME2, but the published CobiT materials also have a similar limited set of CMMI maturity level guidance materials for each of their internal controls. Although summarized at a very high level, these maturity model guidelines allow an enterprise to assess how it is doing with regard to each of CobiT's internal controls.

USING CobiT IN A SOx ENVIRONMENT

When SOx first became effective in the United States, there was little guidance on how to implement and manage its Section 404 internal controls reviews. The Public Company Accounting Oversight Board initially indicated that they were going to establish some specific standards but initially left enterprises and their external auditors on their own. With its heavy emphasis on high-level IT-oriented internal controls, many enterprises adopted CobiT as the internal control framework of choice. This section reviews using the CobiT framework to help achieve SOx compliance.

Chapter 1 discussed SOx Section 404 internal controls assessment requirements and highlighted risk-based approaches for evaluating internal controls with an emphasis on the COSO internal controls framework. CobiT is a powerful alternative internal controls assessment framework, particularly in environments with a heavy concentration of IT processes and resources. As discussed, both COSO internal controls and CobiT use three-dimensional frameworks to describe their internal control environments. Each is similar,

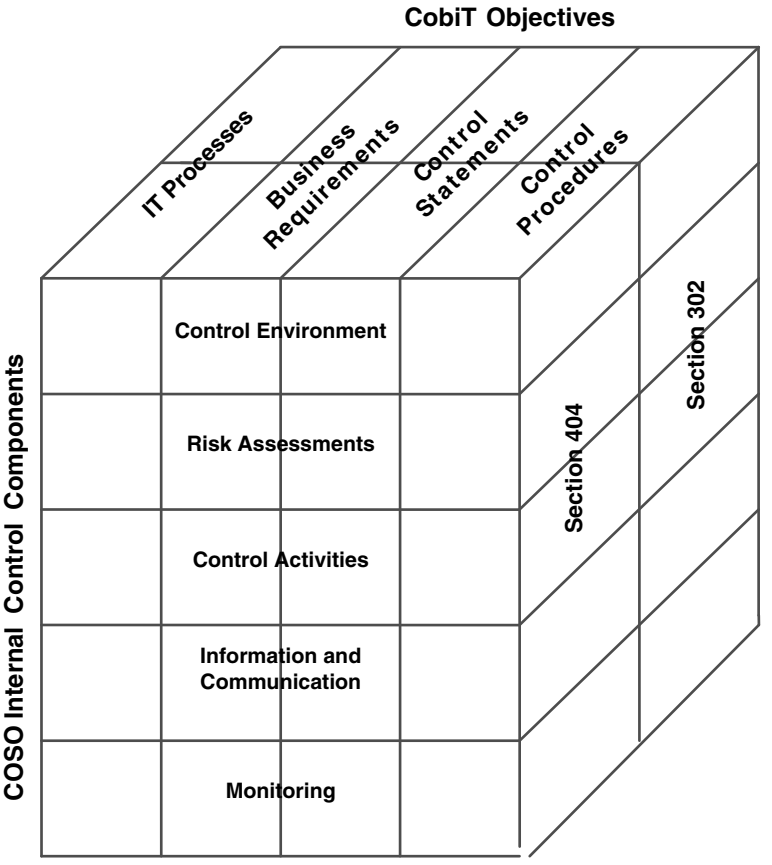

EXHIBIT 2.8 Relationship between COSO Components and CobiT Objectives

but with slight differences in classifications and terminology. Exhibit 2.8 shows how the CobiT framework maps to the COSO internal controls model. CobiT's prime objectives, from Planning and Enterprise to Monitoring and Evaluation, can be used to understand and evaluate internal controls through COSO's five internal control components. Whether considering COSO internal controls in general or when using CobiT, an internal auditor should move through a series processes from planning to performing risk assessments and on to identifying, documenting, and evaluating key internal controls.

With SOx, the industry-wide increased emphasis on IT governance and the recognition of the criticality of IT in most internal control decisions, CobiT has gone through multiple revisions up through its current 4.1 edition. CobiT's sponsoring IT Governance Institute has been doing an excellent job releasing publications that map the CobiT framework to these other standards. For example, a very detailed study maps the CobiT framework to SOx audit requirements.[4] Exhibit 2.9 is an extract of this published CobiT guidance showing how major CobiT control objective areas links with the major COSO components of internal control. This link-up ties together even better by going a level lower. For example, CobiT objective AI6, Managing Changes, under the Acquire and

	COSCO Components				
	Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring
Plan & Organize COSO Control Objective					
Define a strategic IT plan		X		X	X
Define the information architecture			X	X	
Determine technological direction					
Define the IT organization and relationships	X			X	
Manage the IT investment					
Communicate management aims and directions	X			X	X
Manage human resources	X			X	
Ensure compliance with external relationships			X	X	X
Assess risks		X			
Manage projects					
Manage quality	X		X	X	X
Acquire and Implement COSO Control Objective					
Identify automated solutions					
Acquire and maintain application software			X		
Acquire and maintain technology infrastructure			X		
Develop and maintain procedures			X	X	
Install and accredit			X		
Manage changes			X		X
Deliver and Support COSO Control Objective					
Define and manage service levels	X		X		X
Manage third-party services	X	X	X		X
Manage performance and capacity	X		X		
Ensure continuous service	X		X		X
Ensure systems security	X		X	X	X
Identify and allocate costs	X		X	X	X
Educate and train users	X		X		
Assist and advise customers					
Manage the configuration	X		X	X	
Manage problems and incidents			X	X	X
Manage data			X	X	
Manage facilities			X		
Manage operations			X	X	
Monitor and Evaluate COSO Control Objective					
Monitor the processes				X	X
Assess internal control adequacy					X
Obtain independent assurance	X				X
Provide for independent audit					

EXHIBIT 2.9 COSO and CobiT Relationships

Implement control domain impacts the COSO components of Control Activities and Monitoring. The current published CobiT detailed control objectives tie to each of these COSO components and the current version of CobiT is in draft form at this time of publication.

There is a close relationship between these CobiT and COSO control objectives and components.

The full set of CobiT control objectives materials will provide strong support for an internal auditor performing a SOx Section 404 internal controls assessment review. Although the concepts can be used in any internal control area, the emphasis is on IT applications and processes. For many enterprises, an understanding and assessment of those IT-associated internal controls is key to achieving SOx compliance. CobiT has been around for some years now, but too many have viewed it as just a specialized IT audit tool, and not a more general help for other internal audit work. Although CobiT's emphasis continues to be on IT, all internal auditors should explore the CobiT framework as a tool for helping with current and evolving SOx compliance requirements.

CobiT ASSURANCE FRAMEWORK GUIDANCE

The CobiT framework provides guidance for establishing effective internal controls with an emphasis on IT resources. In 2008 the ITGI released its Information Technology Assurance Framework (ITAF™)[5] guidance, a good-practice-setting model to provide guidance on the design, conduct, and reporting of IT audit and assurance assignments. The objective of this guidance is to establish standards that address IT audit and assurance professional roles and responsibilities; knowledge and skills; and diligence, conduct, and reporting requirements. This new CobiT guidance focuses on another perhaps soon to be common audit-related word, *assurance.*

This term is also found in IIA basic references that state: ''Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes.'' Assurance services cover all forms of internal auditing, risk management, and compliance services. This CobiT guidance covers a wide range of reviews performed by an internal auditor.

The overall objective of ITAF is to define a set of standards to help ensure the quality, consistency, and reliability of IT assessments, based on a set of good-practice-setting guidelines and procedures. Although the ITAF document refers to its guidance as ''standards,'' CobiT's ISACA professional organization is not recognized as widely as the IIA's International Standards for the Professional Practice of Internal Auditing. Chapter 3 outlines the IIA Standards and summarizes the CobiT-related ITAF Standards. We mention the new ITAF Standards to highlight the fact that internal auditing standards are being developed to help with reviews in a CobiT environment. However, internal auditors should understand that ITAF is new; and it may achieve more recognition as it becomes better accepted and perhaps fine-tuned.

CobiT IN PERSPECTIVE

Whether operational, financial, or IT specialists, all internal auditors should have at least a high-level understanding of the CobiT framework. It is a particularly useful tool for assessing internal controls in a more IT-oriented environment—the type of environment that we almost always encounter today. The decision to use CobiT in internal audits should not be a one-time or individual audit–level decision. Rather, internal audit should train key members of the audit team in the use of CobiT and then try using it to assess internal controls on some other audit currently being developed and documented using the IT audit techniques discussed in Chapters 8 and 10.

Unfortunately, the IIA hasn't really given proper reference to CobiT and its IIA members. Although the IIA now has some good internal audit standards for its members, as discussed in Chapter 3, the IIA Standards do not come close to CobiT as a tool for helping to define and understand IT controls. All IT auditors should understand and use CobiT.

If internal audit feels that CobiT will offer some improvements to ongoing audit processes, the concept should first be discussed with the audit committee to explain reasons for changing internal audit approaches. If the enterprise places a heavy reliance on IT systems and processes, using CobiT seems to be a good logistical move. However, an overall internal audit function should avoid having IT internal audit specialists use CobiT assessment processes while the rest of internal audit uses established operational/financial internal audit standards.

CobiT is an elegant—sometimes even too elegant—internal control framework and evaluation tool for assessing internal controls. Perhaps the largest impediment to its overall use is that CobiT was originally constructed as primarily an IT audit tool. Although the move from ISACA to the ITGI sponsorship has broadened its appeal and focus, the published CobiT guidance materials have a very heavy IT focus. This focus sometimes scares away some potential users.

The real strength of CobiT is its IT governance focus, as described in Exhibit 2.1. That exhibit illustrates the importance of the strategic alliance of business and IT resources with value delivery, resource management, risk management, and performance measurement processes. All five of these areas allow an enterprise to establish effective IT governance, and CobiT should help in managing and understanding these concepts. We can expect CobiT published standards and practices to continue to broaden and go beyond just ''IT audit'' special concepts. All internal auditors should learn to use and understand the CobiT internal controls assessment framework.

NOTES

1. IT Governance Institute, *CobiT—Governance, Control and Audit for Information and Related Technology*, 4th ed. (Rolling Meadows, IL: Author, 2000).
2. IT Governance Institute, *CobiT 4.1* (Rolling Meadows, IL: Author, 2007).
3. Capability Maturity Model® Integration (CMMI) is a Carnegie Mellon University–developed process improvement approach that provides organizations with the essential