

COBIT® STUDENT BOOK



Provides high-quality educational material on CobIT® and its implementations that can be integrated into curricula on information systems management, information security management, auditing, information systems auditing or accounting information systems

IT Governance Institute®

The IT Governance Institute (ITGI) (www.itgi.org) was established in 1998 to advance international thinking and standards in directing and controlling an enterprise's information technology. Effective IT governance helps ensure that IT supports business goals, optimises business investment in IT, and appropriately manages IT-related risks and opportunities. The IT Governance Institute offers symposia, original research and case studies to assist enterprise leaders and boards of directors in their IT governance responsibilities.

Information Systems Audit and Control Association®

With more than 35,000 members in more than 100 countries, the Information Systems Audit and Control Association (ISACA®) (www.isaca.org) is a recognised worldwide leader in IT governance, control, security and assurance. Founded in 1969, ISACA sponsors international conferences, publishes the *Information Systems Control Journal*®, develops international information systems auditing and control standards, and administers the globally respected Certified Information Systems Auditor™ (CISA®) designation, earned by more than 35,000 professionals since inception, and the Certified Information Security Manager® (CISM®) designation, a groundbreaking credential earned by 5,000 professionals in its first two years.

Disclaimer

The IT Governance Institute, Information Systems Audit and Control Association [the "Owner(s)"] and the authors have designed and created *COBIT in Academia* and its related publications, titled COBIT® *Caselets*, COBIT® *Student Book*, COBIT® *Case Study: TIBO* and COBIT® *Presentation Package*, (the "Work"), primarily as an educational resource for educators. The Owners make no claim that use of any of the Work will assure a successful outcome. The Work should not be considered inclusive of any proper information, procedures and tests or exclusive of other information, procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific information, procedure or test, the educator should apply his/her own professional judgement to the specific circumstances presented by the particular systems or information technology environment.

Disclosure

Copyright © 2004 IT Governance Institute. All rights reserved. This publication is intended solely for academic use and shall not be used in any other manner (including for any commercial purpose). Reproductions of selections of this publication are permitted solely for the use described above and must include the following copyright notice and acknowledgement: "Copyright © 2004 IT Governance Institute. All rights reserved. Reprinted by permission." *COBIT in Academia* may not otherwise be used, copied, or reproduced, in any form by any means (electronic, mechanical, photocopying, recording or otherwise), without the prior written permission of the IT Governance Institute. Any modification, distribution, performance, display, transmission, or storage, in any form by any means (electronic, mechanical, photocopying, recording or otherwise) of *COBIT in Academia* is strictly prohibited. No other right or permission is granted with respect to this work.

IT Governance Institute

3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 USA
Phone: +1.847.590.7491
Fax: +1.847.253.1443
E-mail: research@isaca.org
Web sites: www.itgi.org and www.isaca.org

ISBN 1-893209-96-2

COBIT in Academia

Printed in the United States of America

ACKNOWLEDGEMENTS

IT GOVERNANCE INSTITUTE WISHES TO RECOGNISE:**The Board of Trustees**

Marios Damianides, CISA, CISM, CA, CPA, Ernst & Young LLP, USA, International President
 Abdul Hamid Bin Abdullah, CISA, CPA, Auditor General's Office, Singapore, Vice President
 William C. Boni, CISM, Motorola, USA, Vice President
 Ricardo Bria, CISA, SAFE Consulting Group, Spain, Vice President
 Everett C. Johnson, CPA, Deloitte & Touche LLP (retired), USA, Vice President
 Howard Nicholson, CISA, CRN Solutions, Australia, Vice President
 Bent Poulsen, CISA, CISM, VP Securities Services, Denmark, Vice President
 Frank K. M. Yam, CISA, CIA, CCP, CFE, Focus Strategic Group Inc., Hong Kong, Vice President
 Robert S. Roussey, CPA, University of Southern California, USA, Past International President
 Paul A. Williams, FCA, MBCS, Paul Williams Consulting, UK, Past International President
 Emil D'Angelo, CISA, CISM, Bank of Tokyo-Mitsubishi, USA, Trustee
 Ronald Saull, CSP, Great-West Life and IMG Financial, Canada, Trustee
 Erik Guldentops, CISA, CISM, Belgium, Advisor, IT Governance Institute

The Development Team

Erik Guldentops, CISA, CISM, University of Antwerp Management School, Belgium (Chair)
 Roger Debreceny, Ph.D., FCPA, University of Hawaii, USA
 Steven De Haes, University of Antwerp Management School, Belgium (Project Manager)
 Roger Lux, Farmers Insurance Group, USA
 John Mitchell, CISA, CIA, CFE, LHS Business Control, UK
 Ed O'Donnell, Ph.D., Arizona State University, USA
 Scott Summers, Ph.D., Brigham Young University, USA
 Wim Van Grembergen, Ph.D., University of Antwerp Management School, Belgium

The Review Team

Georges Ataya, CISA, CISM, CISSP, Solvay Business School, Belgium
 Janie Chang, Ph.D., San Jose State University, USA
 Frederick Gallegos, CISA, CGFM, CDE, California State Polytechnic University at Pomona, USA

TABLE OF CONTENTS

Purpose of This Document	5
Chapter 1: The COBIT Framework	6
COBIT Context: Emergence of Enterprise and IT Governance	6
COBIT Audience: Management, Users and Auditors	9
COBIT Framework Specifics	9
COBIT Family of Products	16
COBIT Business Objective Orientation	20
COBIT Summary Table	21
Review Questions	22
Chapter 2: COBIT Components for IT Process DS2	23
COBIT Framework Navigation	23
Concept and Importance of DS2 <i>Manage Third-party Services</i>	24
Control Objectives for DS2 <i>Manage Third-party Services</i>	25
Control Practices for DS2 <i>Manage Third-party Services</i>	28
Audit Guidelines for DS2 <i>Manage Third-party Services</i>	30
Management Guidelines for DS2 <i>Manage Third-party Services</i>	34
Review Questions	37
Chapter 3: COBIT Components	38
PO1 Define a Strategic Information Technology Plan (control objectives only)	39
PO9 <i>Assess Risks</i>	50
PO10 <i>Manage Projects</i>	61
AI2 <i>Acquire and Maintain Application Software</i>	77
DS5 <i>Ensure Systems Security</i>	92
DS6 <i>Identify and Allocate Costs</i>	111
M1 <i>Monitor the Processes</i>	120
M2 <i>Assess Internal Control Adequacy</i>	128

Bold titles are contained in this sample.

PURPOSE OF THIS DOCUMENT

The goal of the *Student Book* is to provide high-quality educational material on COBIT and its implementations that can be integrated into curricula for students in information systems management, information security management, auditing, information systems auditing or accounting information systems. It was developed by the IT Governance Institute, in collaboration with a group of international academics and practitioners.

The *Student Book* is composed of three parts. Chapter 1 explains all the aspects of the COBIT framework in detail. Chapter 2 takes this knowledge one level further by discussing in detail how the elements of the COBIT framework can be applied, specifically for managing third-party services (COBIT process DS2). Both chapters 1 and 2 provide numerous examples and testimonials that illustrate the COBIT framework and its use in practice. Chapter 3 provides the COBIT elements for eight of the 34 COBIT processes (as selected by the authors of this book): PO1, PO9, PO10, AI2, DS5, DS6, M1 and M2. The information in chapter 3 can be used by students as guidance while working on specific COBIT exercises.

The IT Governance Institute has also developed three other products that can accompany this COBIT *Student Book*: the COBIT Presentation Package, providing a comprehensive 80-slide PowerPoint deck explaining all the COBIT elements; the COBIT *Case Study: TIBO* (graduate level), which can be used by students to apply the COBIT knowledge in a real-life situation; and COBIT *Caselets*, which are some minicases for smaller exercises at the undergraduate level.

SAMPLE

CHAPTER 1: THE COBIT FRAMEWORK

In recent years, it has become increasingly evident that there is a need for a reference framework for developing and managing internal controls and appropriate levels of security in information technology (IT). The application of IT has become central to the strategy and business processes of many entities. As such, successful organisations require an appreciation for and a basic understanding of the risks and constraints of IT at all levels within the enterprise in order to achieve effective direction and adequate controls. COBIT (*Control Objectives for Information and related Technology*) provides such a control and security framework for IT. The COBIT framework is explained in this chapter.

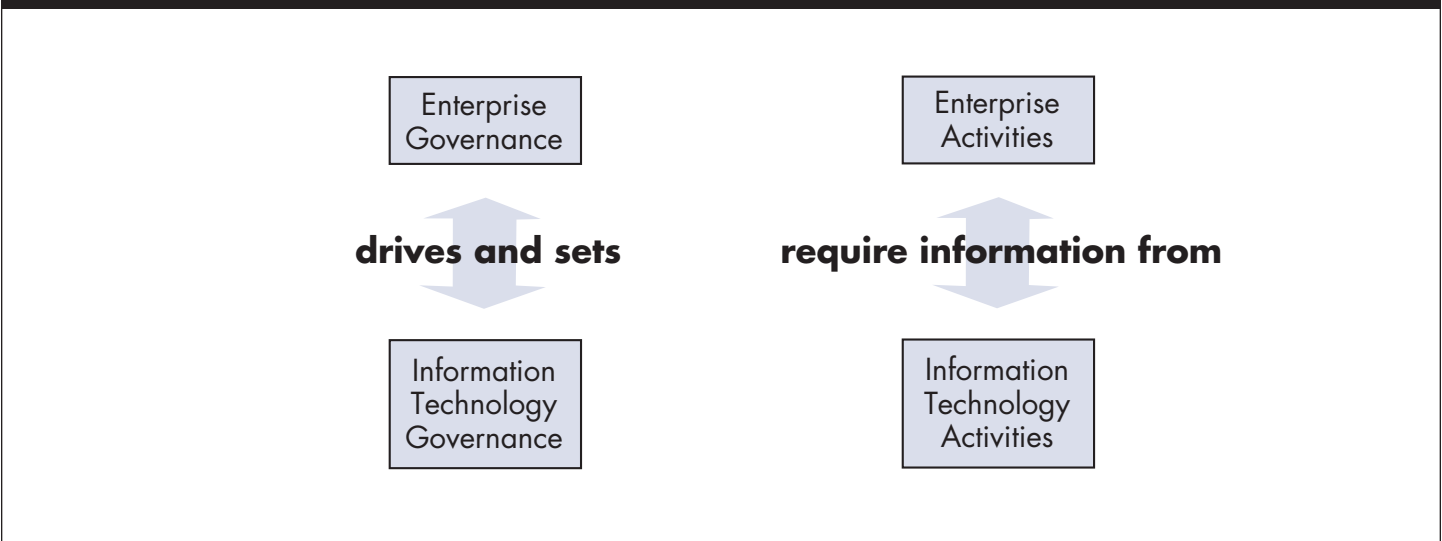
COBIT CONTEXT: EMERGENCE OF ENTERPRISE AND IT GOVERNANCE

Information technology is an important factor in achieving success in the information economy and central to an entity’s operational and financial management. As a result, enterprise governance and IT governance can no longer be considered separate and distinct disciplines. Effective enterprise governance focuses individual and group expertise and experience where it can be most productive, monitors and measures performance, and provides assurance to critical issues. IT, long considered solely an enabler of an enterprise’s strategy, must now be regarded as an integral part of that strategy.

IT governance provides the structure that links IT processes, IT resources and information to enterprise strategies and objectives. IT governance integrates and institutionalises optimal ways of planning and organising, acquiring and implementing, delivering and supporting, and monitoring and evaluating IT performance. IT governance is integral to the success of enterprise governance by assuring efficient and effective measurable improvements in related enterprise processes. IT governance enables the enterprise to take full advantage of its information, thereby maximising benefits, capitalising on opportunities and gaining competitive advantage.

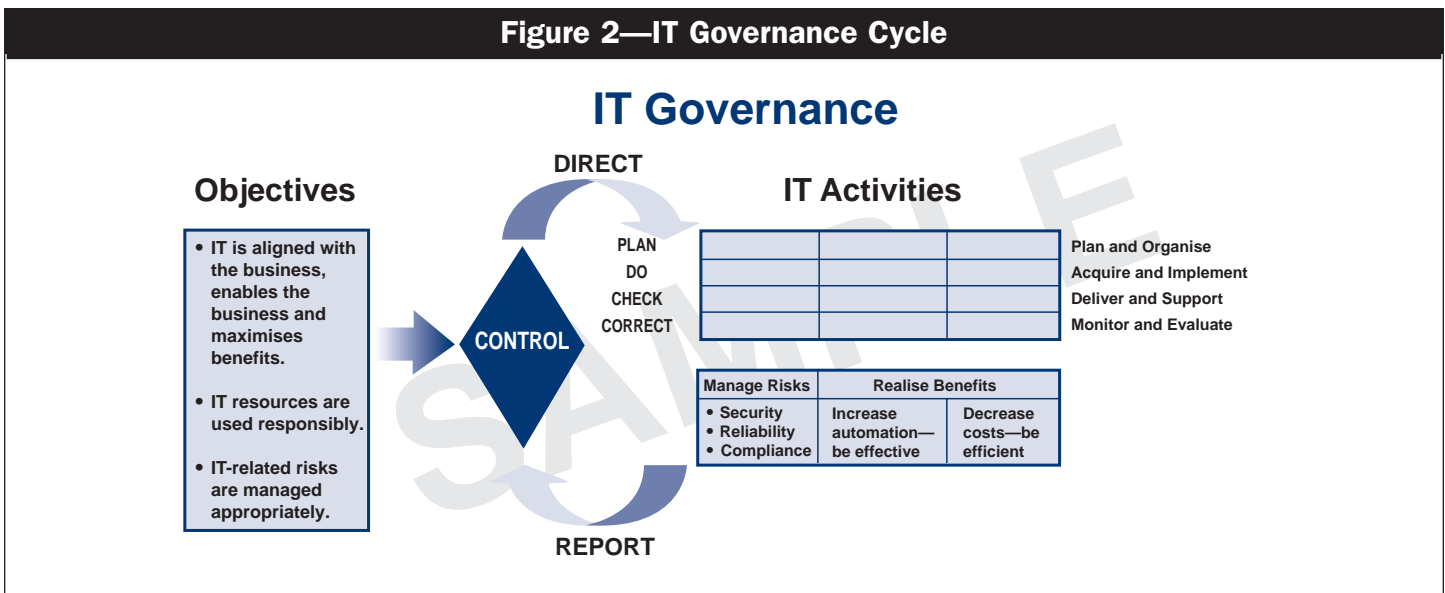
Looking at the interplay of enterprise and IT governance processes in more detail (**figure 1**), enterprise governance, the system by which entities are directed and controlled, drives and sets IT governance. At the same time, IT should provide critical input to, and constitute an important component of, strategic plans. IT may in fact influence strategic opportunities outlined by the enterprise.

Figure 1—Enterprise Governance and IT Governance



Well-managed enterprises employ generally accepted best practices to ensure that the enterprise is achieving its strategic and operational goals. Achieving those goals requires an entity to take on some level of risk—there can be no reward without some level of risk. The entity institutes controls over strategy and operations to manage its risk and assist in the achievement of its goals and strategies. From these objectives flows the organisation’s direction, which dictates certain enterprise activities, using the enterprise’s resources. The results of the enterprise activities are measured and reported on, providing input to the constant revision and maintenance of the controls, beginning the cycle again.

The management of IT is also governed by best practices to ensure that the enterprise’s information and related technology support its business objectives, its resources are used responsibly and its risks are managed appropriately. These practices form a basis for direction of IT activities, which can be characterised as plan and organise, acquire and implement, deliver and support, and monitor and evaluate, for the dual purposes of managing risks (to gain security, reliability and compliance) and realising benefits (increasing effectiveness and efficiency). Reports are issued on the outcomes of IT activities, which are measured against the various practices and controls, and then the cycle begins again. This cycle is illustrated in **figure 2**.

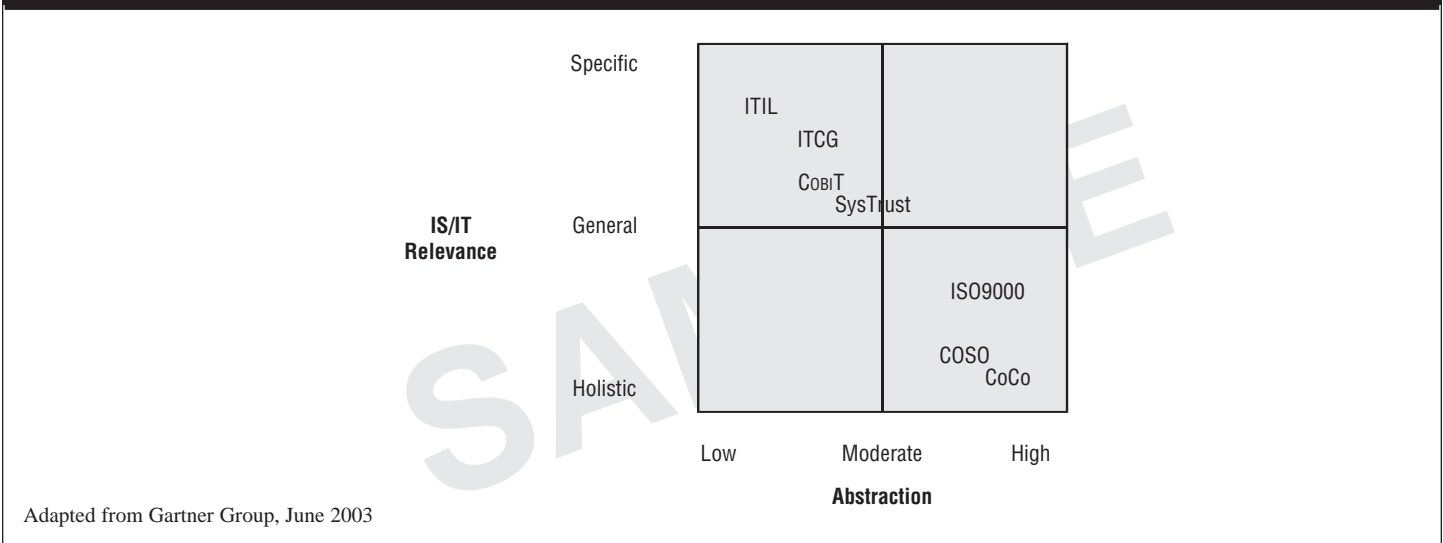


In view of these ongoing changes, the development of this framework for IT control objectives and the continued applied research in IT controls, based on this framework, are cornerstones for effective progress in the field of information and related technology controls.

Overall business control models, such as COSO (Committee of Sponsoring Organisations of the Treadway Commission, *Internal Control—Integrated Framework*, 1992, the *COSO Enterprise Risk Management Framework*, 2004) in the US, Turnbull in the UK, CoCo in Canada and King in South Africa have been developed and published. As well, a number of IT-only control models exist, such as the Security Code of Conduct from the Department of Trade and Industry (DTI), UK, Information Technology Control Guidelines from the Canadian Institute of Chartered Accountants (CICA), Canada, and the Security Handbook from the National Institute of Standards and Technology (NIST), USA. However, these focused control models do not provide a comprehensive and usable control model over IT that is in support of business processes. The purpose of COBIT is to bridge this gap by providing a foundation that is closely linked to business objectives while focusing on IT.

Most closely related to COBIT from an IT perspective is the *SysTrust™ Principles and Criteria* for systems reliability. SysTrust is an authoritative issuance of both the Assurance Services Executive Committee of the American Institute of Certified Public Accountants (AICPA) in the US and the Assurance Services Development Board of CICA in Canada, based in part on the COBIT control objectives. SysTrust is designed to increase the comfort of management, customers and business partners with the systems that support a business or a particular activity. The SysTrust service entails the public accountant providing an assurance service in which he/she evaluates and tests whether a system is reliable when measured against four essential principles: availability, security, integrity and maintainability. Other control and governance models are mapped in **figure 3**; they include IT Infrastructure Library (ITIL), Information Technology Control Guidelines (ITCG), International Organisation for Standardisation’s ISO9000, COSO report (a report on *Internal Control—An Integrated Framework*, sponsored by COSO) and Criteria of Control (CoCo), published by the CICA.

Figure 3—Models of Control and Governance



The main focus of COBIT is the development of clear policies and good practices for security and control in IT for worldwide endorsement by commercial, governmental and professional organisations. Its primary goal is the development of control objectives primarily from the business objectives and needs perspective. This approach is compliant with the COSO perspective, which is first and foremost a management framework for internal controls. Subsequently, audit objectives and guidelines were developed from the control objectives (certification of financial information, certification of internal control measures, efficiency and effectiveness, etc.) perspective.

Pages 9 through 21 deleted from this sample.

REVIEW QUESTIONS

1. How does the cycle of plan, do, check and correct relate to IT governance?
2. Describe the similarities and differences between CoCo or COSO and COBIT. Could an entity employ both CoCo or COSO *and* COBIT? Should an entity employ both CoCo or COSO *and* COBIT?
3. Describe the target audience of COBIT.
4. Describe the seven information criteria that COBIT is designed to address.
5. Discuss the five IT resources recognised by the COBIT framework.
6. What is the difference between an audit guideline and a management guideline? Why should there be separate guidelines in the COBIT framework?
7. What is the difference between the general concept of control and control in the IT environment?
8. Give two examples of IT domains and explain each.
9. What is the difference between a key goal indicator and a key performance indicator?
10. What is a maturity model? Invent a maturity model for a knowledge domain outside of information technology (e.g., for a student, sports or cultural activity or organisation).
11. What is an IT process? Give two examples of IT processes.

CHAPTER 2: COBIT COMPONENTS FOR IT PROCESS DS2

The objective of this chapter is to demonstrate how to use the COBIT framework. It begins with a navigational outline of the COBIT framework, which shows how to navigate through the COBIT product set. Next, all the COBIT components of the COBIT process DS2 *manage third-party services* are explained and linked to each other.

COBIT FRAMEWORK NAVIGATION

The COBIT framework defines 34 IT processes divided into four IT domains: Plan and Organise (PO), Acquire and Implement (AI), Deliver and Support (DS), and Monitor and Evaluate (M). For each of the 34 IT processes, COBIT provides control objectives, control practices, management guidelines and audit guidelines.

For each IT process, the high-level control objectives section presents control statements, business requirements, enablers and considerations. The domain indicator (“PO” for Plan and Organise, “AI” for Acquire and Implement, “DS” for Deliver and Support, and “M” for Monitor and Evaluate) is shown at top left in this high-level control objective section. The applicable information criteria and IT resources managed are shown in **figures 15** and **16**.

The remainder of this chapter, focused on *manage third-party services*, is organised as follows:

- Concept and importance of the process
- Control objective
- Control practice
- Audit guidelines
- Management guidelines
- Chapter review questions

Figure 15—COBIT Waterfall

The COBIT framework has been limited to high-level control objectives in the form of a business need within a particular IT process, the achievement of which is enabled by a control statement, for which consideration should be given to potentially applicable controls.

The control objectives have been organised by process/activity, but navigation aids have been provided not only to facilitate entry from any one vantage point, but also to facilitate combined or

global approaches, such as installation/implementation of a process, global management responsibilities for a process and the use of IT resources by a process.

It should also be noted that the control objectives have been defined in a generic way, i.e., not depending on the technical platform, while accepting the fact that some special technology environments may need separate coverage for control objectives.

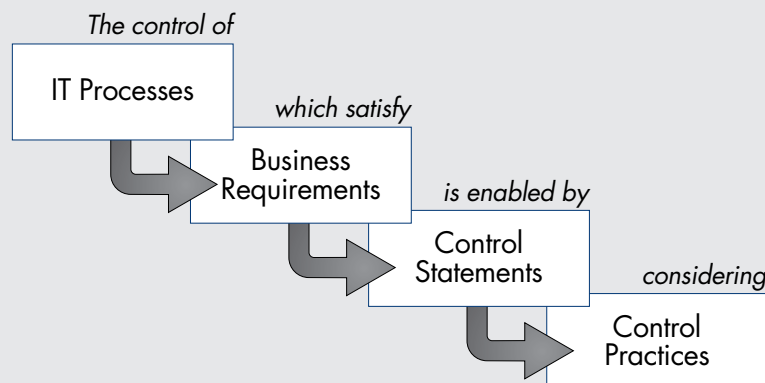
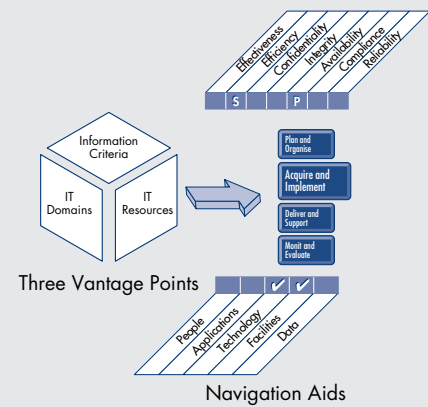


Figure 16—COBIT Navigation Aids

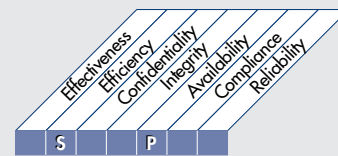
To facilitate efficient use of the control objectives in support of the different vantage points, some navigation aids are provided as part of the presentation of the high-level control objectives. For each of the three dimensions along which the COBIT framework can be approached—processes, IT resources and information criteria—a navigation aid is provided.



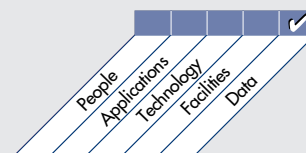
IT domains are identified by this icon in the UPPER RIGHT CORNER of each page in the control objectives section, with the domain under review highlighted and enlarged.



The cue to information criteria is provided in the UPPER LEFT CORNER in the control objectives section by means of this matrix, which identifies which criteria are applicable to each high-level control objective and to which degree (primary or secondary).



A second matrix in the LOWER RIGHT CORNER in the control objectives section identifies the IT resources that are specifically managed by the process under consideration—not those that merely take part in the process. For example, the *manage data* process concentrates particularly on integrity and reliability of the data resource.



Pages 25 through 37 deleted from this sample.

CHAPTER 3: COBIT COMPONENTS

This chapter contains all the COBIT components (control objectives, control practices, audit guidelines and management guidelines) of a selected group of COBIT processes:

- PO1—figures 22-25
- PO9—figures 26-29
- PO10—figures 30-33
- AI2—figures 34-37
- DS5—figures 38-41
- DS6—figures 42-45
- M1—figures 46-49
- M2—figures 50-53

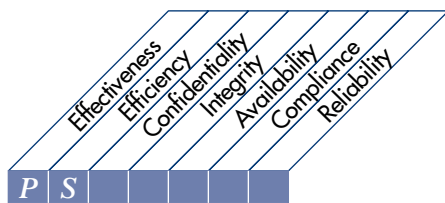
SAMPLE

Figure 22—Control Objectives for Define a Strategic Information Technology Plan

HIGH-LEVEL CONTROL OBJECTIVE

PO1 Plan and Organise

Define a Strategic Information Technology Plan



Control over the IT process of

defining a strategic IT plan

that satisfies the business requirement

to strike an optimum balance of information technology opportunities and IT business requirements as well as ensuring its further accomplishment

is enabled by

a strategic planning process undertaken at regular intervals giving rise to long-term plans; the long-term plans should periodically be translated into operational plans setting clear and concrete short-term goals

and takes into consideration

- Enterprise business strategy
- Definition of how IT supports the business objectives
- Inventory of technological solutions and current infrastructure
- Monitoring the technology markets
- Timely feasibility studies and reality checks
- Existing systems assessments
- Enterprise position on risk, time-to-market and quality
- Need for senior management buy-in, support and critical review



Figure 22—Control Objectives for Define a Strategic Information Technology Plan

DETAILED CONTROL OBJECTIVES

1 DEFINE A STRATEGIC INFORMATION TECHNOLOGY PLAN

1.1 IT as Part of the Organisation’s Long- and Short-range Plan

CONTROL OBJECTIVE

Senior management is responsible for developing and implementing long- and short-range plans that fulfill the organisation’s mission and goals. In this respect, senior management should ensure that IT issues as well as opportunities are adequately assessed and reflected in the organisation’s long- and short-range plans. IT long- and short-range plans should be developed to help ensure that the use of IT is aligned with the mission and business strategies of the organisation.

1.2 IT Long-range Plan

CONTROL OBJECTIVE

IT management and business process owners are responsible for regularly developing IT long-range plans supporting the achievement of the organisation’s overall missions and goals. The planning approach should include mechanisms to solicit input from relevant internal and external stakeholders impacted by the IT strategic plans. Accordingly, management should implement a long-range planning process, adopt a structured approach and set up a standard plan structure.

**1.3 IT Long-range Planning—
Approach and Structure**

CONTROL OBJECTIVE

IT management and business process owners should establish and apply a structured approach regarding the long-range planning process. This should result in a high-quality plan that covers the basic questions of what, who, how, when and why. The IT planning process should take into account risk assessment results, including business, environmental, technology and human resources risks. Aspects that need to be taken

into account and adequately addressed during the planning process include the organisational model and changes to it, geographical distribution, technological evolution, costs, legal and regulatory requirements, requirements of third parties or the market, planning horizon, business process reengineering, staffing, in- or outsourcing, data, application systems and technology architectures. Benefits of the choices made should be clearly identified. The IT long- and short-range plans should incorporate performance indicators and targets. The plan itself should also refer to other plans, such as the organisation quality plan and the information risk management plan.

1.4 IT Long-range Plan Changes

CONTROL OBJECTIVE

IT management and business process owners should ensure that a process is in place to modify the IT long-range plan in a timely and accurate manner to accommodate changes to the organisation’s long-range plan and changes in IT conditions. Management should establish a policy requiring that IT long- and short-range plans are developed and maintained.

1.5 Short-range Planning for the IT Function

CONTROL OBJECTIVE

IT management and business process owners should ensure that the IT long-range plan is regularly translated into IT short-range plans. Such short-range plans should ensure that appropriate IT function resources are allocated on a basis consistent with the IT long-range plan. The short-range plans should be reassessed periodically and amended as necessary in response to changing business and IT conditions. The timely performance of feasibility studies should ensure that the execution of the short-range plans is adequately initiated.

continued on next page

Figure 22—Control Objectives for Define a Strategic Information Technology Plan (cont.)**1.6 Communication of IT Plans***CONTROL OBJECTIVE*

Management should ensure that IT long- and short-range plans are communicated to business process owners and other relevant parties across the organisation.

1.7 Monitoring and Evaluating of IT Plans*CONTROL OBJECTIVE*

Management should establish processes to capture and report feedback from business process owners and users regarding the quality and usefulness of long- and short-range plans. The feedback obtained should be evaluated and considered in future IT planning.

1.8 Assessment of Existing Systems*CONTROL OBJECTIVE*

Prior to developing or changing the strategic or long-range IT plan, IT management should assess the existing information systems in terms of degree of business automation, functionality, stability, complexity, costs, strengths and weaknesses to determine the degree to which the existing systems support the organisation's business requirements.

Pages 42 through 135 deleted from this sample.

SAMPLE