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. ITGI offers original research and case studies to assist enterprise leaders and boards of directors in their IT governance responsibilities.

Disclaimer
ITGI and the author of IT Governance Using COBIT® and Val ITTM: Student Book, 2nd Edition have designed the publication primarily as an educational resource for educators. ITGI, ISACA® and the authors make no claim that use of this product will assure a successful outcome. The publication should not be considered inclusive of all proper procedures and tests or exclusive of all proper procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific procedure or test, controls professionals should apply their own professional judgement to the specific control circumstances presented by the particular systems or IT environment. Note that this publication is an update of COBIIT® in Academia: Student Book.

Disclosure
© 2007 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 © 2007 IT Governance Institute. All rights reserved. Reprinted by permission.’ IT Governance Using COBIT® and Val ITTM: Student Book, 2nd Edition 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 ITGI. Any modification, distribution, performance, display, transmission or storage, in any form by any means (electronic, mechanical, photocopying, recording or otherwise) of IT Governance Using COBIT® and Val ITTM: Student Book, 2nd Edition 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: info@itgi.org
Web site: www.itgi.org

ISBN 978-1-60420-024-9
IT Governance Using COBIT® and Val ITTM: Student Book, 2nd Edition
Printed in the United States of America
ACKNOWLEDGEMENTS

ITGI wishes to recognise:

Researcher
Ed O’Donnell, University of Kansas, USA

Contributors
Roger Stephen Debreceny, Ph.D., FCPA, University of Hawaii, USA
Steven DeHaes, University of Antwerp Management School, Belgium
Erik Guldentops, CISA, CISM, University of Antwerp Management School, Belgium
Robert Parker, CISA, CA, CMC, FCA, Canada
V. Sambamurthy, Ph.D., Michigan State University, USA
Scott Lee Summers, Ph.D., Brigham Young University, USA
John Thorp, The Thorp Network, Canada
Wim Van Grembergen, Ph.D., University of Antwerp (UA) and University of Antwerp Management School (UAMS) and IT Alignment and Governance Research Institute (ITAG), Belgium
Ramesh Venkataraman, Ph.D., Indiana University, USA

ITGI Board of Trustees
Everett C. Johnson, CPA, Deloitte & Touche (retired), USA, International President
Georges Ataya, CISA, CISM, CISSP, ICT Control sa-nv, Belgium, Vice President
William C. Boni, CISM, Motorola, USA, Vice President
Lucio Augusto Molina Focazio, CISA, Colombia, Vice President
Avinash Kadam, CISA, CISM, CBCP, CISSP, Miel e-Security Pvt. Ltd., India, Vice President
Jean-Louis Leignel, MAGE Conseil, France, Vice President
Howard Nicholson, CISA, City of Salisbury, Australia, Vice President
Frank Yam, CISA, CIA, CCP, CFE, CFSA, FFA, FHKCS, FH KIoD, Focus Strategic Group, Hong Kong, Vice President
Marios Damianides, CISA, CISM, CA, CPA, Ernst & Young LLP, USA, Past International President
Robert S. Roussey, CPA, University of Southern California, USA, Past International President
Ronald Saull, CSP, Great-West Life Assurance and IGM Financial, Canada, Trustee

IT Governance Committee
Tony Hayes, FCPA, Queensland Government, Australia, Chair
Max Blecher, Virtual Alliance, South Africa
Sushil Chatterji, Singapore
Anil Jogani, CISA, FCA, Tally Solutions Limited, UK
John W. Lainhart, IV, CISA, CISM, CIPP/G, IBM, USA
Romulo Lomparte, CISA, Banco de Credito BCP, Peru
Michael Schirmbrand, Ph.D., CISA, CISM, CPA, KPMG LLP, Austria
Ronald Saull, CSP, Great-West Life Assurance and IGM Financial, Canada

ITGI Advisory Panel
Ronald Saull, CSP, Great-West Life Assurance and IGM Financial, Canada, Chair
Roland Bader, F. Hoffmann-La Roche AG, Switzerland
Linda Betz, IBM Corporation, USA
Jean-Pierre Cormiou, Renault, France
Rob Clyde, CISM, Symantec, USA
Richard Granger, NHS Connecting for Health, UK
Howard Schmidt, CISM, R&H Security Consulting LLC, USA
Alex Siow Yuen Khong, StarHub Ltd., Singapore
Amit Yoran, Yoran Associates, USA
ACKNOWLEDGEMENTS (CONT.)

Academic Relations Committee
Scott Lee Summers, Ph.D., Brigham Young University, USA, Chair
Casey G. Cegielski, Ph.D., CISA, Auburn University, USA
Patrick Hanrion, CISM, CISSP, CNE, MCSE, Microsoft, USA
Donna Hutcheson, CISA, XR Group Inc., USA
Cejka Jiri Josef, CISA, Dipl. El.-Ing., KPMG Fides Peat, Switzerland
Michael Lambert, CISA, CISM, CARRA, Canada
Ed O’Donnell, University of Kansas, USA
Theodore Tryfonas, Ph.D., CISA, University of Glamorgan, Wales
Ramesh Venkataraman, Ph.D., Indiana University, USA

COBIT Steering Committee
Roger Stephen Debreceny, Ph.D., FCPA, University of Hawaii, USA, Chair
Gary S. Baker, CA, Deloitte & Touche, Canada
Steven DeHaes, University of Antwerp Management School, Belgium
Rafael Eduardo Fabius, CISA, Republica AFAP, S.A., Uruguay
Urs Fischer, CISA, CIA, CPA (Swiss), Swiss Life, Switzerland
Erik Guldentops, CISA, CISM, University of Antwerp Management School, Belgium
Gary Hardy, IT Winners, South Africa
Jimmy Heschl, CISM, CISA, KPMG, Austria
Debbie A. Lew, CISA, Ernst & Young LLP, USA
Maxwell J. Shanahan, CISA, FCPA, Max Shanahan & Associates, Australia
Dirk E. Steuperaert, CISA, PricewaterhouseCoopers LLC, Belgium
Robert E. Stroud, CA Inc., USA

ITGI Affiliates and Sponsors
ISACA chapters
American Institute for Certified Public Accountants
ASIS International
The Center for Internet Security
Commonwealth Association of Corporate Governance Inc.
FIDA Inform
Information Security Forum
Information Systems Security Association
Institut de la Gouvernance des Systèmes d’Information
Institute of Management Accountants
ISACA
ITGI Japan
Solvay Business School
University of Antwerp Management School
Aldion Consulting Pte. Ltd.
CA
Hewlett-Packard
IBM
ITpreneurs Nederlands BV
LogLogic Inc.
Phoenix Business and Systems Process Inc.
Project Rx Inc.
Symantec Corporation
Wolcott Group LLC
World Pass IT Solutions
# TABLE OF CONTENTS

1. Purpose of This Document ........................................................................................................................................................................2

2. Governing IT Resources ..................................................................................................................................................................................3
   What Is IT Governance? ............................................................................................................................................................................3
   Why Is IT Governance Important? ..........................................................................................................................................................3
   What Does IT Governance Cover? ..........................................................................................................................................................4
   Conclusion .................................................................................................................................................................................................10

3. Managing IT Risks ..................................................................................................................................................................................11
   The COBIT Framework ............................................................................................................................................................................11
   Conclusion .................................................................................................................................................................................................16

4. Providing IT Assurance ........................................................................................................................................................................17
   Assurance Planning ................................................................................................................................................................................18
   Defining the Scope of the Assurance Initiative .....................................................................................................................................18
   Assurance Initiative Execution ..............................................................................................................................................................19
   Examples of the Use of Detailed Assurance Steps ..................................................................................................................................22
   Conclusion .................................................................................................................................................................................................23

5. Auditing IT Controls Over Financial Reporting .....................................................................................................................................24
   IT Control Environment ...........................................................................................................................................................................24
   Computer Operations ...............................................................................................................................................................................24
   Access to Programs and Data ...............................................................................................................................................................24
   Program Development and Program Change .........................................................................................................................................25
   The Audit Process ...............................................................................................................................................................................25
   Conclusion .................................................................................................................................................................................................31

Appendix—COBIT Components for Five Processes .................................................................................................................................32
   COBIT Framework Navigation ............................................................................................................................................................32
   DS2 COBIT Components With Additional Guidance ..................................................................................................................................33
   PO9 COBIT Components ....................................................................................................................................................................44
   AI2 COBIT Components ....................................................................................................................................................................52
   DS5 COBIT Components ....................................................................................................................................................................65
   ME2 COBIT Components ....................................................................................................................................................................81

COBIT and Related Products ........................................................................................................................................................................90

Underlined titles are contained in this sample.
1. PURPOSE OF THIS DOCUMENT

The goal of IT Governance Using COBIT® and Val IT™: Student Book, 2nd Edition, is to provide high-quality educational material that can be integrated into courses on information systems, management control or assurance services. This document provides overviews of:

- IT governance
- The Control Objectives for Information and related Technology (COBIT®) framework for IT controls
- IT assurance initiatives
- Audits of IT controls over financial reporting

The Student Book, 2nd Edition, was developed by ITGI, in collaboration with a group of international academics and practitioners, by assembling excerpts from other ITGI publications.

The objective in creating this document was to develop a learning resource that can be used effectively by students with little or no business experience. As a result, the ITGI materials reproduced herein have been abridged by removing material that addresses practical and operational issues that are of concern to business people and information technology (IT) professionals, but may be difficult for students to appreciate and comprehend.

Chapter 2, Governing IT Resources, describes IT governance practices and how an organisation can create business value through IT investments. Material for chapter 2 was assembled from the Board Briefing on IT Governance, 2nd Edition and Enterprise Value: Governance of IT Investments—The Val IT Framework. Students will learn how organisations manage IT resources to deliver stakeholder value through strategic alignment, value delivery, risk management and performance measurement. This chapter also describes how organisations can manage their IT investments as a portfolio.

Chapter 3, Managing IT Risks, presents a framework of control objectives designed to help an organisation manage risks that threaten information and related technology. Material for chapter 3 was assembled from COBIT® 4.1. Students will learn how to establish control objectives for planning and organising the IT function, acquiring and implementing IT capabilities, delivering and supporting IT functions, and monitoring and evaluating IT service delivery. This chapter also discusses the role of IT application controls in a risk management initiative.

Chapter 4, Providing IT Assurance, describes the processes that assurance professionals use to evaluate and report on the effectiveness of IT controls. Material for chapter 4 was assembled from the IT Assurance Guide Using COBIT®. Students will learn how to develop a plan for IT assurance initiatives, scope the initiative by identifying key control objectives, and test the design and operating effectiveness of control procedures designed to address key control objectives. This chapter also provides examples of how to test the design and operating effectiveness of IT controls, and evaluate the impact of control weaknesses.

Chapter 5, Auditing IT Controls Over Financial Reporting, outlines the process for auditing IT controls over financial reporting. Material for chapter 5 was assembled from IT Control Objectives for Sarbanes-Oxley, 2nd Edition. Students will learn about the process for auditing IT general controls over financial reporting, including how to plan and scope an evaluation, assess IT risk, document IT controls, evaluate the design and operating effectiveness of IT controls, and build sustainability into the evaluation process.
2. GOVERNING IT RESOURCES

Increasingly, top management is realising the significant impact that IT can have on the success of the enterprise. Management hopes for heightened understanding of the way IT is operated and the likelihood of its being leveraged successfully for competitive advantage. Boards and executive management need to extend governance to IT and provide the leadership, organisational structures and processes that ensure that the enterprise’s IT sustains and extends the enterprise’s strategies and objectives. IT governance is not an isolated discipline; it is an integral part of overall enterprise governance.

The need to integrate IT governance with overall governance is similar to the need for IT to be an integral part of the enterprise rather than something practiced in remote corners or ivory towers. An increasingly educated and assertive set of stakeholders is concerned about the sound management of its interests. This has led to the emergence of governance principles and standards for overall enterprise governance. Furthermore, regulations establish board responsibilities and require that the board of directors exercise due diligence in its roles. Investors have also realised the importance of governance; research shows they are willing to pay a premium of more than 20 percent on shares of enterprises that have shown to have good governance practices in place.1

Enterprise governance is a set of responsibilities and practices exercised by the board and executive management with the goal of providing strategic direction, ensuring that objectives are achieved, ascertaining that risks are managed appropriately and verifying that the enterprise’s resources are used responsibly. While governance developments have primarily been driven by the need for the transparency of enterprise risks and the protection of shareholder value, the pervasive use of technology has created a critical dependency on IT that calls for a specific focus on IT governance.

IT is essential to manage the transactions, information and knowledge necessary to initiate and sustain economic and social activities. In most enterprises, IT has become an integral part of the business and is fundamental to support, sustain and grow the business. Successful enterprises understand and manage the risks and constraints of IT. Increasingly, boards of directors understand the strategic importance of IT and have put IT governance firmly on their agenda.

WHAT IS IT GOVERNANCE?

The overall objective of IT governance is to understand the issues and strategic importance of IT so the enterprise can sustain its operations and implement the strategies required to extend its activities into the future. IT governance aims to ensure that expectations for IT are met and IT risks are mitigated. IT governance is the responsibility of the board of directors and executive management. It is an integral part of enterprise governance and consists of the leadership and organisational structures and processes that ensure that the organisation’s IT sustains and extends the organisation’s strategies and objectives.

At the heart of the governance responsibilities of setting strategy, managing risks, delivering value and measuring performance are the stakeholder values, which drive the enterprise and IT strategy. Sustaining the current business and growing into new business models certainly are stakeholder expectations, and can be achieved only with adequate governance of the enterprise’s IT infrastructure.

The purpose of IT governance is to direct IT endeavors, to ensure that IT’s performance meets the following objectives:

- Alignment of IT with the enterprise and realisation of the promised benefits
- Use of IT to enable the enterprise by exploiting opportunities and maximising benefits
- Responsible use of IT resources
- Appropriate management of IT-related risks

WHY IS IT GOVERNANCE IMPORTANT?

The use of IT has the potential to be the major driver of economic wealth in the 21st century. Whilst IT is already critical to enterprise success, provides opportunities to obtain a competitive advantage and offers a means for increasing productivity, it will do all this to an even greater extent in the future. Successfully leveraging IT to transform the enterprise and create value-added products and services has become a universal business competency. IT is fundamental for managing enterprise resources, dealing with suppliers and customers, and enabling increasingly global transactions.

1 McKinsey’s Investors Opinion Survey, June 2000

Pages 4 through 10 deleted from this sample.
3. MANAGING IT RISKS

For many enterprises, information and the technology that supports it represent their most valuable, but often least understood, assets. Successful enterprises recognise the benefits of information technology and use it to drive their stakeholders’ value. These enterprises also understand and manage the associated risks, such as increasing regulatory compliance and critical dependence of many business processes on IT. Managing risks requires a framework for control over IT that fits with and supports the Committee of Sponsoring Organisations of the Treadway Commission (COSO) Internal Control—Integrated Framework, the widely accepted control framework for enterprise governance and risk management, and similar compliant frameworks.

COBIT provides good practices across a domain and process framework, and presents activities in a manageable and logical structure. COBIT’s good practices represent the consensus of experts. They are strongly focused on control and less so on execution. These practices will help optimise IT-enabled investments, ensure service delivery and provide a measure against which to judge when things do go wrong.

The business orientation of COBIT consists of linking business goals to IT goals, providing metrics and maturity models to measure their achievement, and identifying the associated responsibilities of business and IT process owners. The process focus of COBIT is illustrated by a process model that subdivides IT into 34 processes in line with the responsibility areas of plan, build, run and monitor, providing an end-to-end view of IT. Operational management uses processes to organise and manage ongoing IT activities. COBIT provides a generic process model that represents all the processes normally found in IT functions, providing a common reference model understandable to operational IT and business managers.

To achieve effective governance, executives expect controls to be implemented by operational managers within a defined control framework for all IT processes. COBIT’s IT control objectives are organised by IT process; therefore, the framework provides a clear link amongst IT governance requirements, IT processes and IT controls. The COBIT process model has been mapped to IT governance focus areas, providing a bridge between what operational managers need to execute and what executives wish to govern.

In summary, COBIT is a framework and supporting tool set that allow managers to bridge the gap with respect to control requirements, technical issues and business risks, and communicate that level of control to stakeholders. COBIT enables the development of clear policy and good practice for IT control throughout enterprises. COBIT is continuously kept up to date and harmonised with other standards. Hence, COBIT has become the integrator for IT best practices and the umbrella framework for IT governance that helps in understanding and managing the risks and benefits associated with IT. The process structure of COBIT and its high-level business-oriented approach provide an end-to-end view of IT and the decisions to be made about IT.

THE COBIT FRAMEWORK

Governance and control frameworks are becoming a part of IT management best practice and are an enabler for establishing IT governance and complying with continually increasing regulatory requirements. IT best practices have become significant due to a number of factors:

• Business managers and boards demanding a better return from IT investments and concern over the generally increasing amount of IT expenditures
• The need to meet regulatory requirements for IT controls in areas such as financial reporting and in specific sectors such as finance, pharmaceutical and healthcare
• The selection of service providers and the management of service outsourcing and acquisition
• Increasingly complex IT-related risks, such as network security
• IT governance initiatives that include adoption of control frameworks and best practices to help monitor and improve critical IT activities to increase business value and reduce business risk
• The need for enterprises to assess how they are performing against generally accepted standards and against their peers (benchmarking)

Business orientation is the main theme of COBIT. It is designed to be employed not only by IT service providers, users and auditors, but also as comprehensive guidance for management and business process owners. Defining a set of generic business and IT goals provides a more refined basis for establishing business requirements and developing the metrics that allow measurement against these goals. Every enterprise uses IT to enable business initiatives, and these can be represented as business goals for IT. Once the goals have been defined, they need to be monitored to ensure that actual delivery matches expectations. This is achieved by metrics derived from the goals and captured in an IT scorecard that the customer can understand and follow, and that enables the provider to focus on its own internal objectives.
The IT organisation delivers against these goals by a clearly defined set of processes that use people skills and technology infrastructure to run automated business applications whilst leveraging business information. These resources, together with the processes, constitute an enterprise architecture for IT. To respond to the business requirements for IT, the enterprise needs to invest in the resources required to create an adequate technical capability [e.g., an enterprise resource planning (ERP) system] to support a business capability (e.g., implementing a supply chain) resulting in the desired outcome (e.g., increased sales and financial benefits). The IT resources identified in COBIT can be defined as follows:

- **Applications** are the automated user systems and manual procedures that process the information.
- **Information** is the data in all their forms input, processed and output by the information systems, in whatever form is used by the business.
- **Infrastructure** is the technology and facilities (hardware, operating systems, database management systems, networking, multimedia, etc., and the environment that houses and supports them) that enable the processing of the applications.
- **People** are the personnel required to plan, organise, acquire, implement, deliver, support, monitor and evaluate the information systems and services. They may be internal, outsourced or contracted as required.

COBIT defines IT activities in a generic process model within four domains. A process model encourages process ownership, enabling responsibilities and accountability to be defined. To govern IT effectively, it is important to appreciate the activities and risks within IT that need to be managed. These can be summarised as follows.

**Plan and Organise (PO)**

This domain covers strategy and tactics, and concerns the identification of the way IT can best contribute to the achievement of the business objectives. The realisation of the strategic vision needs to be planned, communicated and managed for different perspectives. A proper organisation as well as technological infrastructure should be put in place. This domain typically addresses the following management questions:

- Are IT and the business strategy aligned?
- Is the enterprise achieving optimum use of its resources?
- Does everyone in the organisation understand the IT objectives?
- Are IT risks understood and being managed?
- Is the quality of IT systems appropriate for business needs?

**Acquire and Implement (AI)**

To realise the IT strategy, IT solutions need to be identified, developed or acquired, as well as implemented and integrated into the business process. In addition, changes in and maintenance of existing systems are covered by this domain to make sure the solutions continue to meet business objectives. This domain typically addresses the following management questions:

- Are new projects likely to deliver solutions that meet business needs?
- Are new projects likely to be delivered on time and within budget?
- Will the new systems work properly when implemented?
- Will changes be made without upsetting current business operations?

**Deliver and Support (DS)**

This domain is concerned with the actual delivery of required services, which includes service delivery, management of security and continuity, service support for users, and management of data and the operational facilities. It typically addresses the following management questions:

- Are IT services being delivered in line with business priorities?
- Are IT costs optimised?
- Is the workforce able to use the IT systems productively and safely?
- Are adequate confidentiality, integrity and availability in place?

**Monitor and Evaluate (ME)**

All IT processes need to be regularly assessed over time for their quality and compliance with control requirements. This domain addresses performance management, monitoring of internal control, regulatory compliance and providing governance. It typically addresses the following management questions:

- Is IT’s performance measured to detect problems before it is too late?
Does management ensure that internal controls are effective and efficient?
Can IT performance be linked back to business goals?
Are risk, control, compliance and performance measured and reported?

In more detail, the overall COBIT framework can be shown graphically as in figure 3, with COBIT’s process model of four domains containing 34 generic processes, managing the IT resources to deliver information to the business according to business and governance requirements. Descriptions of each control objective across the four domains are provided in appendix 1.

**Controls-based**

COBIT defines control objectives for all 34 processes, as well as overarching process and application controls. Control is defined as the policies, procedures, practices and organisational structures designed to provide reasonable assurance that business objectives will be achieved and undesired events will be prevented (or detected and corrected). IT control objectives provide a complete set of high-level requirements to be considered by management for effective control of each IT process. Control objectives are statements of managerial actions to increase value or reduce risk and are designed to provide reasonable assurance that business objectives will be achieved and undesired events will be prevented (or detected and corrected).

The enterprise’s system of internal controls impacts IT at three levels:

- At the executive management level, business objectives are set, policies are established, and decisions are made on how to deploy and manage the resources of the enterprise to execute the enterprise strategy. The overall approach to governance and control is established by the board and communicated throughout the enterprise. The IT control environment is directed by this top-level set of objectives and policies.

- At the business process level, controls are applied to specific business activities. Most business processes are automated and integrated with IT application systems, resulting in many of the controls at this level being automated as well. These controls are known as application controls. However, some controls within the business process remain as manual procedures, such as authorisation for transactions, separation of duties and manual reconciliations. Therefore, controls at the business process level are a combination of manual controls operated by the business and automated business and application controls. Both are the responsibility of the business to define and manage, although the application controls require the IT function to support their design and development.

- To support the business processes, IT provides IT services, usually in a shared service to many business processes, as many of the development and operational IT processes are provided to the whole enterprise, and much of the IT infrastructure is provided as a common service (e.g., networks, databases, operating systems and storage). The controls applied to all IT service activities are known as IT general controls. The reliable operation of these general controls is necessary for reliance to be placed on application controls. For example, poor change management could jeopardise (accidentally or deliberately) the reliability of automated integrity checks.

Effective controls reduce risk, increase the likelihood of value delivery, and improve efficiency because there will be fewer errors and a more consistent management approach. To achieve effective governance, controls need to be implemented by operational managers within a defined control framework for all IT processes. Since COBIT’s IT control objectives are organised by IT process, the framework provides clear links amongst IT governance requirements, IT processes and IT controls. Each of COBIT’s IT processes has a process description and a number of control objectives. As a whole, they are the characteristics of a well-managed process.

**IT General Controls and Application Controls**

General controls are controls embedded in IT processes and services. Examples include systems development, change management, security and computer operations. Controls embedded in business process applications are commonly referred to as application controls. Examples include completeness, accuracy, validity, authorisation and segregation of duties.

COBIT assumes the design and implementation of automated application controls to be the responsibility of IT, which are covered in the Acquire and Implement domain. The operational management and control responsibility for application controls is not with IT, but with the business process owner. Hence, the responsibility for application controls is an end-to-end joint responsibility between business and IT. The business is responsible to properly define functional and control requirements, and use automated services. IT is responsible to automate and implement business functional and control requirements, and establish controls to maintain the integrity of applications controls. Therefore, the COBIT IT processes cover general IT controls, but only the development aspects of application controls;
responsibility for definition and operational usage is with the business. The following list provides a recommended set of application control objectives:

- **AC1 Source Data Preparation and Authorisation**—Ensure that source documents are prepared by authorised and qualified personnel, following established procedures, taking into account adequate segregation of duties regarding the origination and approval of these documents. Errors and omissions can be minimised through good input form design. Errors and irregularities must be detected so they can be reported and corrected.

- **AC2 Source Data Collection and Entry**—Establish that data input is performed in a timely manner by authorised and qualified staff members. Correction and resubmission of data that were erroneously input are performed without compromising original transaction authorisation levels. Where appropriate for reconstruction, original source documents should be retained for the appropriate amount of time.
• AC3 Accuracy, Completeness and Authenticity Checks—Ensure that transactions are accurate, complete and valid. Validate and edit, or send back for correction, input data as close to the point of origination as possible.
• AC4 Processing Integrity and Validity—Maintain the integrity and validity of data throughout the processing cycle. Detection of erroneous transactions should not disrupt the processing of valid transactions.
• AC5 Output Review, Reconciliation and Error Handling—Establish procedures and associated responsibilities to ensure that the necessary control information is provided and used to enable verification, detection and correction of the accuracy of output.
• AC6 Transaction Authentication and Integrity—Before passing transaction data between internal applications and business or operational functions (in or outside the enterprise), check for proper addressing, authenticity of origin and integrity of content. Maintain authenticity and integrity during transmission or transport.

**Measurement-driven**

A basic need for every enterprise is to understand the status of its own IT systems and to decide what level of management and control the enterprise should provide. To decide on the right level, management should ask: How far should we go, and is the cost justified by the benefit? Obtaining an objective view of an enterprise’s own performance level is not easy. Enterprises need to establish goals and metrics to measure where they are and where improvement is required, and implement a management tool kit to monitor this improvement.

Goals and metrics are defined in COBIT at three levels:

• IT goals and metrics that define what the business expects from IT and how to measure it
• Process goals and metrics that define what the IT process must deliver to support IT’s objectives and how to measure it
• Activity goals and metrics that establish what needs to happen inside the process to achieve the required performance and how to measure it

Goals are defined top-down in that a business goal will determine a number of IT goals to support it. An IT goal is achieved by one process or the interaction of a number of processes. Therefore, IT goals help define the different process goals. In turn, each process goal requires a number of activities, thereby establishing the activity goals.

COBIT uses two types of metrics:

• Outcome measures, previously key goal indicators (KGIs), indicate whether the goals have been met. These can be measured only after the fact and, therefore, are called ‘lag indicators’.
• Performance indicators, previously key performance indicators (KPIs), indicate whether goals are likely to be met. They can be measured before the outcome is clear and, therefore, are called ‘lead indicators’.

Outcome measures define measures that inform management—after the fact—whether an IT function, process or activity has achieved its goals. The outcome measures of the IT functions are often expressed in terms of information criteria:

• Availability of information needed to support the business needs
• Absence of integrity and confidentiality risks
• Cost-efficiency of processes and operations
• Confirmation of reliability, effectiveness and compliance

Performance indicators define measures that determine how well the business, IT function or IT process is performing in enabling the goals to be reached. They are lead indicators of whether goals will likely be reached, thereby driving the higher-level goals. They often measure the availability of appropriate capabilities, practices and skills, and the outcome of underlying activities. For example, a service delivered by IT is a goal for IT, but a performance indicator and a capability for the business. This is why performance indicators are sometimes referred to as performance drivers, particularly in balanced scorecards.

Therefore, the metrics provided are both an outcome measure of the IT function, IT process or activity goal they measure, and a performance indicator driving the higher-level business, IT function or IT process goal.

**Figure 4** illustrates the relationship amongst the business, IT, process and activity goals, and the different metrics. From top left to top right, the goals cascade is illustrated. Below the goal is the outcome measure for the goal. The small arrow indicates that the same metric is a performance indicator for the higher-level goal.

**CONCLUSION**

And pages 16 through 21 deleted from the sample.
EXAMPLES OF THE USE OF DETAILED ASSURANCE STEPS

The following sections provide illustrative examples of how the assurance testing steps could be applied.

**Testing of Control Design**

**Situation:** General computer controls review in a transaction processing organisation; assessment of the COBIT process AI6 Manage Changes; COBIT control objective AI6.2 Impact assessment, prioritisation and authorisation

**Observations:** For the selected systems (e.g., application, platform or network), the assurance professional inventoried the types of changes that can be implemented, procedures (formal or informal) currently in place, all parties involved in the change management process, tools used, etc. This was done through interviews with involved persons and enquiries for documented procedures. The result of this work was a comprehensive and correct flowchart of the change management process.

The assurance professional reviewed the identified process flow to determine whether there was a step defined in the procedure to assess the impact of a change by a competent person or group of persons. The assurance professional observed that the template for requesting and approving changes included a section on impact assessment. However, the change management procedure did not mention that this information is mandatory, and the absence of this information did not lead to a rejection of the change request. In addition, the procedure did not mention any documentation standards or required verification and approval steps for the impact assessment.

**Test Result:** The design of this control is flawed, because a fundamental component of the control, i.e., impact assessment, is incomplete at best. It is possible that changes are implemented without proper risk assessment, which can lead to unplanned and difficult-to-contain operational disruptions or malfunctions.

**Testing for the Effectiveness of the Control**

**Situation:** General computer controls review in a transaction processing organisation; assessment of the COBIT process AI6 Manage Changes; COBIT control objective AI6.3 Emergency changes

**Observations:** As part of the evaluation of the control design, the assurance professional identified that, for all relevant change management procedures, there is a control defined to help ensure that emergency change requests are reintroduced into the normal change management cycle. In addition, the assurance professional found that there is a procedure that ensures that all emergency changes are appropriately logged in a change management tool.

As part of the control effectiveness testing, a sample of emergency change requests was selected from the change management tool and traced to their reintroduction as normal changes. This tracing included verification of whether the emergency change was actually introduced again as a normal change and whether it was processed following the normal change management procedure.
The assurance professional observed that from the sample of 25 emergency changes selected, three were not subsequently reprocessed as normal changes. In addition, the assurance professional found that from the 22 emergency changes that had been duly reintroduced, only 10 were discussed at the change management board—or at least that there was a trace available that indicated that the 10 changes were discussed (trace included information stored in the change management tool).

**Test Result:** The emergency change procedure is not effective for two reasons:
- Not all emergency changes are reintroduced in the system, leading to a risk of losing emergency changes from sight and not learning from them.
- Emergency changes that have been reintroduced are most likely inadequately discussed and documented, leading to the same risk.

**Documenting the Impact of Control Weaknesses**

**Situation:** General computer controls review in a transaction processing organisation; assessment of the COBIT process AI6 Manage Changes; COBIT control objective AI6.3 Emergency changes

**Observations:** Using the situation as described, the assurance professional needed to gain additional information and perform further analysis to assess and document the impact of the control weaknesses. For the aforementioned examples, the assurance professional needed to consider the types and numbers of changes affected by the control weaknesses.

Some of the required information might/should already be gathered at the planning stage. This information should be used to evaluate the materiality of the weaknesses noted. Notably, the changes affected should be mapped back to the relevant infrastructure components and the applications/information they support/process. In addition, SLA penalties might apply. Analysis of problems noted in the past can help establish the real potential impact of the weaknesses noted.

In this case, it turns out, after discussion with the responsible change manager and confirmation with other change management board members, that the missing emergency changes relate to non-critical systems, and that the missing documentation was only a documentation issue, whereas the actual change, its cause and consequences had, indeed, been discussed but were not formally documented.

**Test Result:** Although the control weaknesses remain as they have been observed, further analysis and documentation showed that the weaknesses were of a lesser importance than originally assessed.

**CONCLUSION**

And pages 23 through 31 deleted from this sample.
APPENDIX—COBIT COMPONENTS FOR FIVE IT PROCESSES

COBIT’s good practices are strongly focused on controls that will help ensure effective service delivery. To achieve effective governance, executives expect controls to be implemented by operational managers within a defined control framework for all IT processes. COBIT’s IT control objectives are organised by IT process to provide a clear link among IT governance requirements and IT controls. The complete COBIT 4.1 publication is posted for download on www.isaca.org/cobit.

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 (ME). For each of the 34 IT processes, COBIT provides control objectives and management guidelines, control practices and IT assurance guidelines.

Each IT process section presents control statements, business requirements, enablers and considerations. The domain indicator (PO, AI, DS and ME) is shown at top left in this IT process section. The applicable information criteria and IT resources managed are shown in figure 7.

DS2 is used as an example and the components for eight additional COBIT processes follow.

Figure 7—COBIT Navigation

Within each IT process, control objectives are provided as generic action statements of the minimum management good practices to ensure that the process is kept under control.
DS2 COBIT COMPONENTS WITH ADDITIONAL GUIDANCE

The navigational outline of the COBIT framework shows how to navigate through the COBIT product set. All of the COBIT components of the COBIT process DS2 Manage third-party services are explained and linked to each other.

Pages 33 through 89 deleted from this sample.
COBIT AND RELATED PRODUCTS

The COBIT framework, in versions 4.0 and higher, includes all of the following:

• Framework—Explains how COBIT organises IT governance, management and control objectives and good practices by IT domains and processes, and links them to business requirements
• Process descriptions—Include 34 IT processes covering the IT responsibility areas from beginning to end
• Control objectives—Provide generic best practice management objectives for IT processes
• Management guidelines—Offer tools to help assign responsibility, measure performance, and benchmark and address gaps in capability
• Maturity models—Provide profiles of IT processes describing possible current and future states

In the years since its inception, COBIT’s core content has continued to evolve, and the number of COBIT-based derivative works has increased. Following are the publications currently derived from COBIT:

• Board Briefing on IT Governance, 2nd Edition—Designed to help executives understand why IT governance is important, what its issues are and what their responsibility is for managing it
• COBIT® Online—Allows users to customise a version of COBIT for their own enterprise, then store and manipulate that version as desired. It offers online, real-time surveys; frequently asked questions; benchmarking; and a discussion facility for sharing experiences and questions.
• COBIT® Control Practices: Guidance to Achieve Control Objectives for Successful IT Governance, 2nd Edition—Provides guidance on the risks to be avoided and value to be gained from implementing a control objective, and instruction on how to implement the objective. Control practices are strongly recommended for use with the IT Governance Implementation Guide: Using COBIT® and Val IT™, 2nd Edition.
• IT Assurance Guide: Using COBIT®—Provides guidance on how COBIT can be used to support a variety of assurance activities and offers suggested testing steps for all the COBIT IT processes and control objectives. It replaces the information in the Audit Guidelines for auditing and self-assessment against the control objectives in COBIT 4.1.
• IT Control Objectives for Sarbanes-Oxley: The Role of IT in the Design and Implementation of Internal Control Over Financial Reporting, 2nd Edition—Provides guidance on how to assure compliance for the IT environment based on the COBIT control objectives
• IT Governance Implementation Guide: Using COBIT® and Val IT™, 2nd Edition—Provides a generic road map for implementing IT governance using COBIT and Val IT resources and offers a supporting tool kit
• COBIT® Quickstart—Provides a baseline of control for the smaller organisation and a possible first step for the larger enterprise
• COBIT® Security Baseline—Focuses on essential steps for implementing information security within the enterprise
• COBIT mappings—Currently posted at www.isaca.org/downloads:
  - Aligning COBIT®, ITIL and ISO 17799 for Business Benefit
  - COBIT® Mapping: Overview of International IT Guidance, 2nd Edition
  - COBIT® Mapping: Mapping of CMMI® for Development V1.2 With COBIT® 4.0
  - COBIT® Mapping: Mapping of ISO/IEC 17799:2005 With COBIT® 4.0
  - COBIT® Mapping: Mapping of ITIL With COBIT® 4.0
  - COBIT® Mapping: Mapping of PMBOK With COBIT® 4.0
  - COBIT® Mapping: Mapping of PRINCE2 With COBIT® 4.0
  - COBIT® Mapping: Mapping of SEI’s CMM for Software With COBIT® 4.0
  - COBIT® Mapping: Mapping of TOGAF 8.1 With COBIT® 4.0


Val IT is the umbrella term used to describe the publications and future additional products and activities addressing the Val IT framework.

Current Val IT-related publications are:
• Enterprise Value: Governance of IT Investments—The Val IT™ Framework, which explains how an enterprise can extract optimal value from IT-enabled investments and is based on the COBIT framework. It is organised into:
  - Three processes—Value Governance, Portfolio Management and Investment Management
  - IT key management practices—Essential management practices that positively influence the achievement of the desired result or purpose of a particular activity. They support the Val IT processes and play roughly the same role as COBIT’s control objectives.
• Enterprise Value: Governance of IT Investments—The Business Case, which focuses on one key element of the investment management process
• Enterprise Value: Governance of IT Investments—The ING Case Study, which describes how a global financial services company manages a portfolio of IT investments in the context of the Val IT framework

For the most complete and up-to-date information on COBIT, Val IT and related products, case studies, training opportunities, newsletters, and other framework-specific information, visit www.isaca.org/cobit and www.isaca.org/valit.