IT
GOVERNANCE
INSTITUTE®

LEADING THE IT GOVERNANCE COMMUNITY

COBIT®

4.1
Excerpt

Executive Summary

Framework

The 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, electronic resources and case studies to assist enterprise leaders and boards of directors in their IT governance responsibilities.

Disclaimer

ITGI (the "Owner") has designed and created this publication, titled COBIT® 4.1 (the "Work"), primarily as an educational resource for chief information officers (CIOs), senior management, IT management and control professionals. The Owner makes 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, CIOs, senior management, IT management and control professionals should apply their own professional judgement to the specific circumstances presented by the particular systems or IT environment.

Disclosure

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*

COBIT® 4.1
Printed in the United States of America

ACKNOWLEDGEMENTS

IT Governance Institute wishes to recognise:

Expert Developers and Reviewers

Mark Adler, CISA, CISM, CIA, CISSP, Allstate Ins. Co., USA
Peter Andrews, CISA, CITP, MCMI, PJA Consulting, UK
Georges Ataya, CISA, CISM, CISSP, MSCS, PBA, Solvay Business School, Belgium
Gary Austin, CISA, CIA, CISSP, CGFM, KPMG LLP, USA
Gary S. Baker, CA, Deloitte & Touche, Canada
David H. Barnett, CISM, CISSP, Applera Corp., USA
Christine Bellino, CPA, CITP, Jefferson Wells, USA
John W. Beveridge, CISA, CISM, CFE, CGFM, CQA, Massachusetts Office of the State Auditor, USA
Alan Boardman, CISA, CISM, CA, CISSP, Fox IT, UK
David Bonewell, CISA, CISSP-ISSEP, Accomac Consulting LLC, USA
Dirk Bruyndonckx, CISA, CISM, KPMG Advisory, Belgium
Don Canilglia, CISA, CISM, USA
Luis A. Capua, CISM, Sindicatura General de la Nación, Argentina
Boyd Carter, PMP, Elegantsolutions.ca, Canada
Dan Casciano, CISA, Ernst & Young LLP, USA
Sean V. Casey, CISA, CPA, USA
Sushil Chatterji, Edutech, Singapore
Ed Chavennes, Ernst & Young LLP, USA
Christina Cheng, CISA, CISSP, SSCP, Deloitte & Touche LLP, USA
Dharmesh Choksey, CISA, CPA, CISSP, PMP, KPMG LLP, USA
Jeffrey D. Custer, CISA, CPA, CIA, Ernst & Young LLP, USA
Beverly G. Davis, CISA, Federal Home Loan Bank of San Francisco, USA
Peter De Bruyne, CISA, Banksys, Belgium
Steven De Haes, University of Antwerp Management School, Belgium
Peter De Koninck, CISA, CFSA, CIA, SWIFT SC, Belgium
Philip De Picker, CISA, MCA, National Bank of Belgium, Belgium
Kimberly de Vries, CISA, PMP, Zurich Financial Services, USA
Roger S. Debreceny, Ph.D., FCPA, University of Hawaii, USA
Zama Dlamini, Deloitte & Touche LLP, South Africa
Rupert Dodds, CISA, CISM, FCA, KPMG, New Zealand
Troy DuMoulin, Pink Elephant, Canada
Bill A. Durrand, CISA, CISM, CA, Ernst & Young LLP, Canada
Justus Ekeigwe, CISA, MBCS, Deloitte & Touche LLP, USA
Rafael Eduardo Fabius, CISA, Republica AFAP S.A., Uruguay
Urs Fischer, CISA, CIA, CPA (Swiss), Swiss Life, Switzerland
Christopher Fox, ACA, PricewaterhouseCoopers, USA
Bob Frelinger, CISA, Sun Microsystems Inc., USA
Zhiwei Fu, Ph. D, Fannie Mae, USA
Monique Garsoux, Dexia Bank, Belgium
Edson Gin, CISA, CFE, SSCP, USA
Sauvik Ghosh, CISA, CIA, CISSP, CPA, Ernst & Young LLP, USA
Guy Groner, CISA, CIA, CISSP, USA
Erik Guldentops, CISA, CISM, University of Antwerp Management School, Belgium
Gary Hardy, IT Winners, South Africa
Jimmy Heschl, CISA, CISM, KPMG, Austria
Benjamin K. Hsaio, CISA, Federal Deposit Insurance Corp., USA
Tom Hughes, Acumen Alliance, Australia
Monica Jain, CSQA, Covansys Corp., US
Wayne D. Jones, CISA, Australian National Audit Office, Australia
John A. Kay, CISA, USA
Lisa Kinyon, CISA, Countrywide, USA
Rodney Kocot, Systems Control and Security Inc., USA
Luc Kordel, CISA, CISM, CISSP, CIA, RE, RFA, Dexia Bank, Belgium
Linda Kostic, CISA, CPA, USA
John W. Lainhart IV, CISA, CISM, IBM, USA

Philip Le Grand, Capita Education Services, UK.
Elsa K. Lee, CISA, CISM, CSQA, AdvanSoft International Inc., USA
Kenny K. Lee, CISA, CISSP, Countrywide SMART Governance, USA
Debbie Lew, CISA, Ernst & Young LLP, USA
Donald Lorete, CPA, Deloitte & Touche LLP, USA
Addie C.P. Lui, MCSA, MCSE, First Hawaiian Bank, USA
Debra Mallette, CISA, CSSBB, Kaiser Permanente, USA
Charles Mansour, CISA, Charles Mansour Audit & Risk Service, UK
Mario Micallef, CPAA, FIA, National Australia Bank Group, Australia
Niels Thor Mikkelsen, CISA, CIA, Danske Bank, Denmark
John Mitchell, CISA, CFE, CITP, FBCS, FIIA, MIIA, QiCA, LHS Business Control, UK
Anita Montgomery, CISA, CIA, Countrywide, USA
Karl Muise, CISA, City National Bank, USA
Jay S. Munnelly, CISA, CIA, CGFM, Federal Deposit Insurance Corp., USA
Sang Nguyen, CISA, CISSP, MCSE, Nova Southeastern University, USA
Ed O'Donnell, Ph.D., CPA, University of Kansas, USA
Sue Owen, Department of Veterans Affairs, Australia
Robert G. Parker, CISA, CA, CMC, FCA, Robert G. Parker Consulting, Canada
Robert Payne, Trencor Services (Pty) Ltd., South Africa
Thomas Phelps IV, CISA, PricewaterhouseCoopers LLP, USA
Vitor Prisca, CISM, Novabase, Portugal
Martin Rosenberg, Ph.D., IT Business Management, UK
Claus Rosenquist, CISA, TrygVesata, Denmark
Jaco Sadie, Sasol, South Africa
Max Shanahan, CISA, FCPA, Max Shanahan & Associates, Australia
Craig W. Silverthorne, CISA, CISM, CPA, IBM Business Consulting Services, USA
Chad Smith, Great-West Life, Canada
Roger Southgate, CISA, CISM, FCCA, CubeIT Management Ltd., UK
Paula Spinner, CSC, USA
Mark Stanley, CISA, Toyota Financial Services, USA
Dirk E. Steuperaert, CISA, PricewaterhouseCoopers, Belgium
Robert E. Stroud, CA Inc., USA
Scott L. Summers, Ph.D., Brigham Young University, USA
Lance M. Turcato, CISA, CISM, CPA, City of Phoenix IT Audit Division, USA
Wim Van Grembergen, Ph.D., University of Antwerp Management School, Belgium
Johan Van Grieken, CISA, Deloitte, Belgium
Greet Volders, Voquals NV, Belgium
Thomas M. Wagner, Gartner Inc., USA
Robert M. Walters, CISA, CPA, CGA, Office of the Comptroller General, Canada
Freddy Withagels, CISA, Capgemini, Belgium
Tom Wong, CISA, CIA, CMA, Ernst & Young LLP, Canada
Amanda Xu, CISA, PMP, KPMG LLP, USA

ITGI Board of Trustees

Acknowledgements

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

CobiT Steering Committee
Roger Debreceny, Ph.D., FCPA, University of Hawaii, USA, Chair
Gary S. Baker, CA, Deloitte & Touche, Canada
Dan Casciano, CISA, Ernst & Young LLP, USA
Steven De Haes, University of Antwerp Management School, Belgium
Peter De Koninck, CISA, CFSA, CIA, SWIFT SC, Belgium
Rafael Eduardo Fabius, CISA, República AFAP SA, 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, CISA, CISM, KPMG, Austria
Debbie A. Lew, CISA, Ernst & Young LLP, USA
Maxwell J. Shanahan, CISA, FCPA, Max Shanahan & Associates, Australia
Dirk Steuperaert, CISA, PricewaterhouseCoopers LLC, Belgium
Robert E. Stroud, CA Inc., USA

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 Corniou, 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

ITGI Affiliates and Sponsors
ISACA chapters
American Institute for Certified Public Accountants
ASIS International
The Center for Internet Security
Commonwealth Association of Corporate Governance
FIDA Inform
Information Security Forum
The 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. Lte.
CA
Hewlett-Packard
IBM
LogLogic Inc.
Phoenix Business and Systems Process Inc.
Symantec Corporation
Wolcott Group LLC
World Pass IT Solutions

TABLE OF CONTENTS

Additional content is available in the full volume of COBIT 4.1, which may be downloaded at *www.itgi.org*, or purchased through *www.isaca.org/bookstore*. The additional content includes the following:

Your feedback on COBIT 4.1 is welcomed. Please visit *www.isaca.org/cobitfeedback* to submit comments.

EXECUTIVE OVERVIEW

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 information technology (IT).

The need for assurance about the value of IT, the management of IT-related risks and increased requirements for control over information are now understood as key elements of enterprise governance. Value, risk and control constitute the core of IT governance.

IT governance is the responsibility of executives and the board of directors, and consists of the leadership, organisational structures and processes that ensure that the enterprise's IT sustains and extends the organisation's strategies and objectives.

Furthermore, IT governance integrates and institutionalises good practices to ensure that the enterprise's IT supports the business objectives. IT governance enables the enterprise to take full advantage of its information, thereby maximising benefits, capitalising on opportunities and gaining competitive advantage. These outcomes require a framework for control over IT that fits with and supports the Committee of Sponsoring Organisations of the Treadway Commission's (COSO's) *Internal Control—Integrated Framework*, the widely accepted control framework for enterprise governance and risk management, and similar compliant frameworks.

Organisations should satisfy the quality, fiduciary and security requirements for their information, as for all assets. Management should also optimise the use of available IT resources, including applications, information, infrastructure and people. To discharge these responsibilities, as well as to achieve its objectives, management should understand the status of its enterprise architecture for IT and decide what governance and control it should provide.

Control Objectives for Information and related Technology (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 more on control, less 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.

For IT to be successful in delivering against business requirements, management should put an internal control system or framework in place. The COBIT control framework contributes to these needs by:
- Making a link to the business requirements
- Organising IT activities into a generally accepted process model
- Identifying the major IT resources to be leveraged
- Defining the management control objectives to be considered

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 four domains and 34 processes in line with the responsibility areas of plan, build, run and monitor, providing an end-to-end view of IT. Enterprise architecture concepts help identify the resources essential for process success, i.e., applications, information, infrastructure and people.

In summary, to provide the information that the enterprise needs to achieve its objectives, IT resources need to be managed by a set of naturally grouped processes.

But how does the enterprise get IT under control such that it delivers the information the enterprise needs? How does it manage the risks and secure the IT resources on which it is so dependent? How does the enterprise ensure that IT achieves its objectives and supports the business?

First, management needs control objectives that define the ultimate goal of implementing policies, plans and procedures, and organisational structures designed to provide reasonable assurance that:
- Business objectives are achieved
- Undesired events are prevented or detected and corrected

Second, in today's complex environments, management is continuously searching for condensed and timely information to make difficult decisions on value, risk and control quickly and successfully. What should be measured, and how? Enterprises need an objective measure of where they are and where improvement is required, and they need to implement a management tool kit to monitor this improvement.

Figure 1 shows some traditional questions and the management information tools used to find the responses, but these dashboards need indicators, scorecards need measures and benchmarking needs a scale for comparison.

Figure 1—Management Information

How do responsible managers keep the ship on course?	DASHBOARD	⇨ Indicators?
How can the enterprise achieve results that are satisfactory for the largest possible segment of stakeholders?	SCORECARDS	⇨ Measures?
How can the enterprise be adapted in a timely manner to trends and developments in its environment?	BENCHMARKING	⇨ Scales?

An answer to these requirements of determining and monitoring the appropriate IT control and performance level is COBIT's definition of:

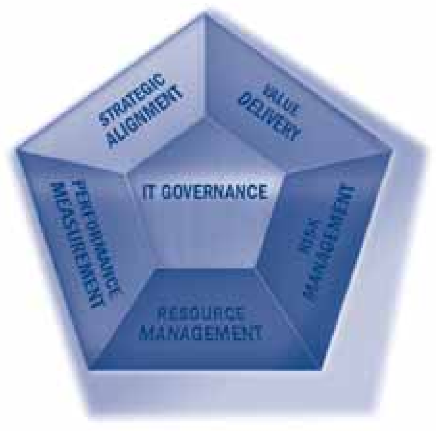
- **Benchmarking** of IT process performance and capability, expressed as maturity models, derived from the Software Engineering Institute's Capability Maturity Model (CMM)
- **Goals and metrics** of the IT processes to define and measure their outcome and performance based on the principles of Robert Kaplan and David Norton's balanced business scorecard
- **Activity goals** for getting these processes under control, based on COBIT's control objectives

The assessment of process capability based on the COBIT maturity models is a key part of IT governance implementation. After identifying critical IT processes and controls, maturity modelling enables gaps in capability to be identified and demonstrated to management. Action plans can then be developed to bring these processes up to the desired capability target level.

Thus, COBIT supports IT governance (**figure 2**) by providing a framework to ensure that:

- IT is aligned with the business
- IT enables the business and maximises benefits
- IT resources are used responsibly
- IT risks are managed appropriately

Figure 2—IT Governance Focus Areas



- **Strategic alignment** focuses on ensuring the linkage of business and IT plans; defining, maintaining and validating the IT value proposition; and aligning IT operations with enterprise operations.
- **Value delivery** is about executing the value proposition throughout the delivery cycle, ensuring that IT delivers the promised benefits against the strategy, concentrating on optimising costs and proving the intrinsic value of IT.
- **Resource management** is about the optimal investment in, and the proper management of, critical IT resources: applications, information, infrastructure and people. Key issues relate to the optimisation of knowledge and infrastructure.
- **Risk management** requires risk awareness by senior corporate officers, a clear understanding of the enterprise's appetite for risk, understanding of compliance requirements, transparency about the significant risks to the enterprise and embedding of risk management responsibilities into the organisation.
- **Performance measurement** tracks and monitors strategy implementation, project completion, resource usage, process performance and service delivery, using, for example, balanced scorecards that translate strategy into action to achieve goals measurable beyond conventional accounting.

Performance measurement is essential for IT governance. It is supported by COBIT and includes setting and monitoring measurable objectives of what the IT processes need to deliver (process outcome) and how to deliver it (process capability and performance). Many surveys have identified that the lack of transparency of IT's cost, value and risks is one of the most important drivers for IT governance. While the other focus areas contribute, transparency is primarily achieved through performance measurement.

These IT governance focus areas describe the topics that executive management needs to address to govern IT within their enterprises. 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. The COBIT process model has been mapped to the IT governance focus areas (see appendix II, Mapping IT Processes to IT Governance Focus Areas, COSO, COBIT IT Resources and COBIT Information Criteria), providing a bridge between what operational managers need to execute and what executives wish to govern.

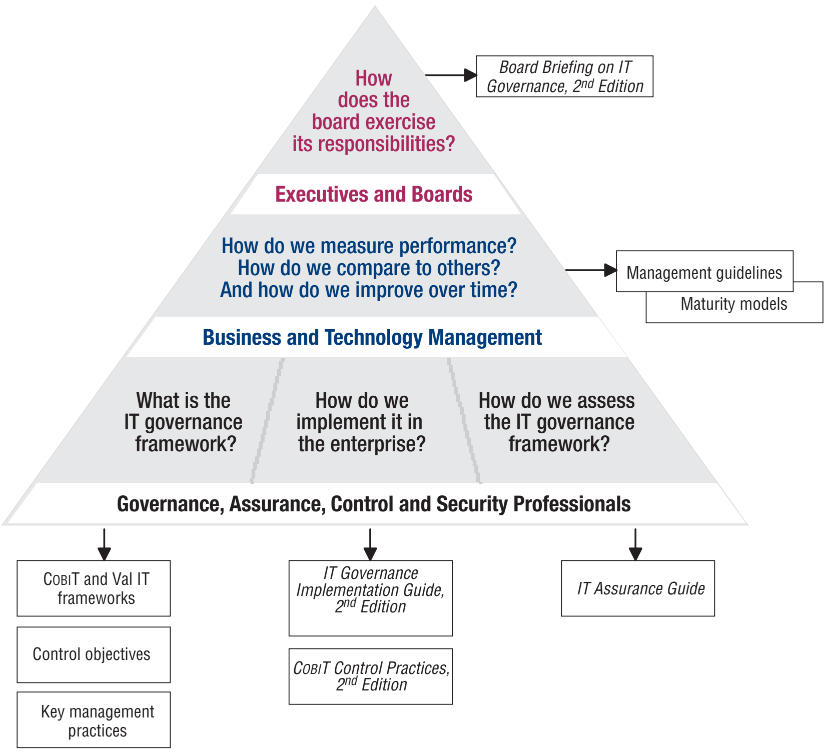
EXECUTIVE OVERVIEW

To achieve effective governance, executives require that controls 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 among IT governance requirements, IT processes and IT controls.

COBIT is focused on what is required to achieve adequate management and control of IT, and is positioned at a high level. COBIT has been aligned and harmonised with other, more detailed, IT standards and good practices (see appendix IV, COBIT 4.1 Primary Reference Material). COBIT acts as an integrator of these different guidance materials, summarising key objectives under one umbrella framework that also links to governance and business requirements.

COSO (and similar compliant frameworks) is generally accepted as the internal control framework for enterprises. COBIT is the generally accepted internal control framework for IT.

Figure 3—COBIT Content Diagram


How does the board exercise its responsibilities?
Board Briefing on IT Governance, 2nd Edition
Executives and Boards
How do we measure performance? How do we compare to others? And how do we improve over time?
Management guidelines
Maturity models
Business and Technology Management
What is the IT governance framework?
How do we implement it in the enterprise?
How do we assess the IT governance framework?
Governance, Assurance, Control and Security Professionals
COBIT and Val IT frameworks
Control objectives
Key management practices
IT Governance Implementation Guide, 2nd Edition
COBIT Control Practices, 2nd Edition
IT Assurance Guide

This COBIT-based product diagram presents the generally applicable products and their primary audience. There are also derived products for specific purposes (*IT Control Objectives for Sarbanes-Oxley, 2nd Edition*), for domains such as security (COBIT *Security Baseline* and *Information Security Governance: Guidance for Boards of Directors and Executive Management*), or for specific enterprises (COBIT *Quickstart* for small and medium-sized enterprises or for large enterprises wishing to ramp up to a more extensive IT governance implementation).

The COBIT products have been organised into three levels (**figure 3**) designed to support:

- Executive management and boards
- Business and IT management
- Governance, assurance, control and security professionals

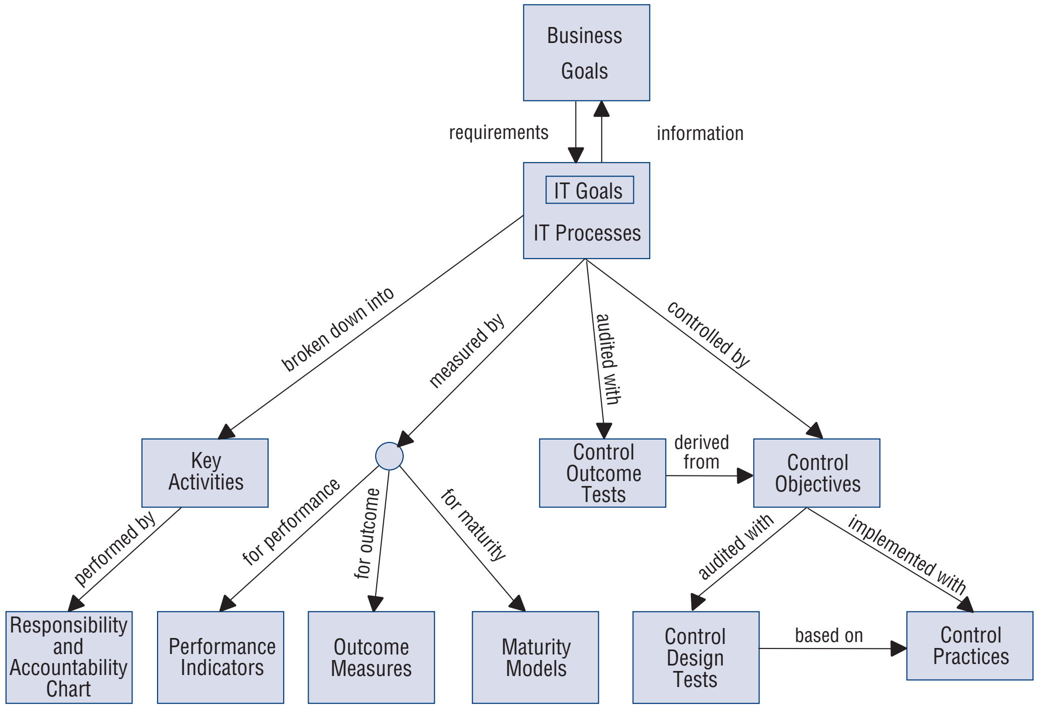
Briefly, the COBIT products include:

- *Board Briefing on IT Governance, 2nd Edition*—Helps executives understand why IT governance is important, what its issues are and what their responsibility is for managing it
- Management guidelines/maturity models—Help assign responsibility, measure performance, and benchmark and address gaps in capability
- Frameworks—Organise IT governance objectives and good practices by IT domains and processes, and link them to business requirements
- Control objectives—Provide a complete set of high-level requirements to be considered by management for effective control of each IT process
- *IT Governance Implementation Guide: Using COBIT® and Val IT™, 2nd Edition*—Provides a generic road map for implementing IT governance using the COBIT and Val IT™ resources
- *COBIT® Control Practices: Guidance to Achieve Control Objectives for Successful IT Governance, 2nd Edition*—Provides guidance on why controls are worth implementing and how to implement them
- *IT Assurance Guide: Using COBIT®*—Provides guidance on how COBIT can be used to support a variety of assurance activities together with suggested testing steps for all the IT processes and control objectives

The COBIT content diagram depicted in **figure 3** presents the primary audiences, their questions on IT governance and the generally applicable products that provide responses. There are also derived products for specific purposes, for domains such as security or for specific enterprises.

All of these COBIT components interrelate, providing support for the governance, management, control and assurance needs of the different audiences, as shown in **figure 4**.

Figure 4—Interrelationships of COBIT Components



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 policies and good practice for IT control throughout enterprises. COBIT is continuously kept up to date and harmonised with other standards and guidance. Hence, COBIT has become the integrator for IT good 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 benefits of implementing COBIT as a governance framework over IT include:
- Better alignment, based on a business focus
- A view, understandable to management, of what IT does
- Clear ownership and responsibilities, based on process orientation
- General acceptability with third parties and regulators
- Shared understanding amongst all stakeholders, based on a common language
- Fulfilment of the COSO requirements for the IT control environment

The rest of this document provides a description of the COBIT framework and all of the core COBIT components, organised by COBIT's four IT domains and 34 IT processes. This provides a handy reference book for all of the main COBIT guidance. Several appendices are also provided as useful references.

The most complete and up-to-date information on COBIT and related products, including online tools, implementation guides, case studies, newsletters and educational materials can be found at *www.isaca.org/cobit*.

COBIT FRAMEWORK

COBIT Mission:
To research, develop, publicise and promote an authoritative, up-to-date, internationally accepted IT governance control framework for adoption by enterprises and day-to-day use by business managers, IT professionals and assurance professionals

THE NEED FOR A CONTROL FRAMEWORK FOR IT GOVERNANCE

A control framework for IT governance defines the reasons IT governance is needed, the stakeholders and what it needs to accomplish.

Why

Increasingly, top management is realising the significant impact that information can have on the success of the enterprise. Management expects heightened understanding of the way IT is operated and the likelihood of its being leveraged successfully for competitive advantage. In particular, top management needs to know if information is being managed by the enterprise so that it is:
- Likely to achieve its objectives
- Resilient enough to learn and adapt
- Judiciously managing the risks it faces
- Appropriately recognising opportunities and acting upon them

Successful enterprises understand the risks and exploit the benefits of IT and find ways to deal with:
- Aligning IT strategy with the business strategy
- Assuring investors and shareholders that a ‘standard of due care’ around mitigating IT risks is being met by the organisation
- Cascading IT strategy and goals down into the enterprise
- Obtaining value from IT investments
- Providing organisational structures that facilitate the implementation of strategy and goals
- Creating constructive relationships and effective communication between the business and IT, and with external partners
- Measuring IT’s performance

Enterprises cannot deliver effectively against these business and governance requirements without adopting and implementing a governance and control framework for IT to:
- Make a link to the business requirements
- Make performance against these requirements transparent
- Organise its activities into a generally accepted process model
- Identify the major resources to be leveraged
- Define the management control objectives to be considered

Furthermore, governance and control frameworks are becoming a part of IT management good practice and are an enabler for establishing IT governance and complying with continually increasing regulatory requirements.

IT good practices have become significant due to a number of factors:
- Business managers and boards demanding a better return from IT investments, i.e., that IT delivers what the business needs to enhance stakeholder value
- Concern over the generally increasing level of IT expenditure
- The need to meet regulatory requirements for IT controls in areas such as privacy and financial reporting (e.g., the US Sarbanes-Oxley Act, Basel II) 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 good practices to help monitor and improve critical IT activities to increase business value and reduce business risk
- The need to optimise costs by following, where possible, standardised, rather than specially developed, approaches
- The growing maturity and consequent acceptance of well-regarded frameworks, such as COBIT, IT Infrastructure Library (ITIL), ISO 27000 series on information security-related standards, ISO 9001:2000 *Quality Management Systems—Requirements*, Capability Maturity Model® Integration (CMMI), Projects in Controlled Environments 2 (PRINCE2) and *A Guide to the Project Management Body of Knowledge* (PMBOK)
- The need for enterprises to assess how they are performing against generally accepted standards and their peers (benchmarking)

Who

A governance and control framework needs to serve a variety of internal and external stakeholders, each of whom has specific needs:

- Stakeholders within the enterprise who have an interest in generating value from IT investments:
  - Those who make investment decisions
  - Those who decide about requirements
  - Those who use IT services
- Internal and external stakeholders who provide IT services:
  - Those who manage the IT organisation and processes
  - Those who develop capabilities
  - Those who operate the services
- Internal and external stakeholders who have a control/risk responsibility:
  - Those with security, privacy and/or risk responsibilities
  - Those performing compliance functions
  - Those requiring or providing assurance services

What

To meet the requirements listed in the previous section, a framework for IT governance and control should:

- Provide a business focus to enable alignment between business and IT objectives
- Establish a process orientation to define the scope and extent of coverage, with a defined structure enabling easy navigation of content
- Be generally acceptable by being consistent with accepted IT good practices and standards and independent of specific technologies
- Supply a common language with a set of terms and definitions that are generally understandable by all stakeholders
- Help meet regulatory requirements by being consistent with generally accepted corporate governance standards (e.g., COSO) and IT controls expected by regulators and external auditors

HOW COBIT MEETS THE NEED

In response to the needs described in the previous section, the COBIT framework was created with the main characteristics of being business-focused, process-oriented, controls-based and measurement-driven.

Business-focused

Business orientation is the main theme of COBIT. It is designed not only to be employed by IT service providers, users and auditors, but also, and more important, to provide comprehensive guidance for management and business process owners.

The COBIT framework is based on the following principle (**figure 5**):

> To provide the information that the enterprise requires to achieve its objectives, the enterprise needs to invest in and manage and control IT resources using a structured set of processes to provide the services that deliver the required enterprise information.

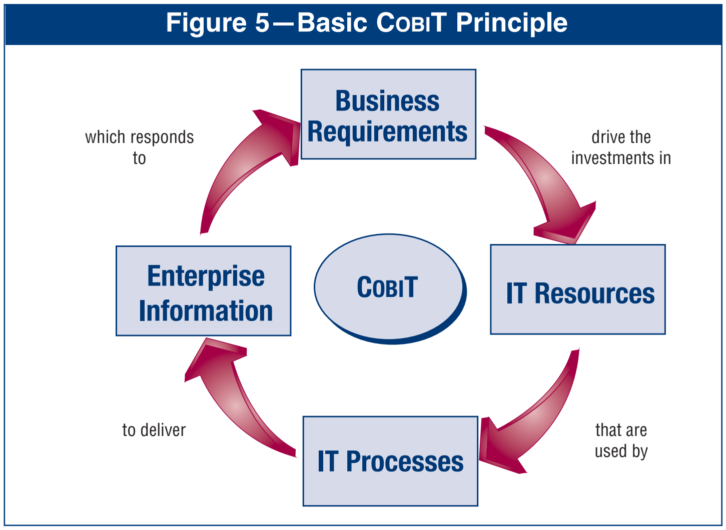
Managing and controlling information are at the heart of the COBIT framework and help ensure alignment to business requirements.

COBIT'S INFORMATION CRITERIA

To satisfy business objectives, information needs to conform to certain control criteria, which COBIT refers to as business requirements for information. Based on the broader quality, fiduciary and security requirements, seven distinct, certainly overlapping, information criteria are defined as follows:

- **Effectiveness** deals with information being relevant and pertinent to the business process as well as being delivered in a timely, correct, consistent and usable manner.

Figure 5—Basic COBIT Principle



- **Efficiency** concerns the provision of information through the optimal (most productive and economical) use of resources.
- **Confidentiality** concerns the protection of sensitive information from unauthorised disclosure.
- **Integrity** relates to the accuracy and completeness of information as well as to its validity in accordance with business values and expectations.
- **Availability** relates to information being available when required by the business process now and in the future. It also concerns the safeguarding of necessary resources and associated capabilities.
- **Compliance** deals with complying with the laws, regulations and contractual arrangements to which the business process is subject, i.e., externally imposed business criteria as well as internal policies.
- **Reliability** relates to the provision of appropriate information for management to operate the entity and exercise its fiduciary and governance responsibilities.

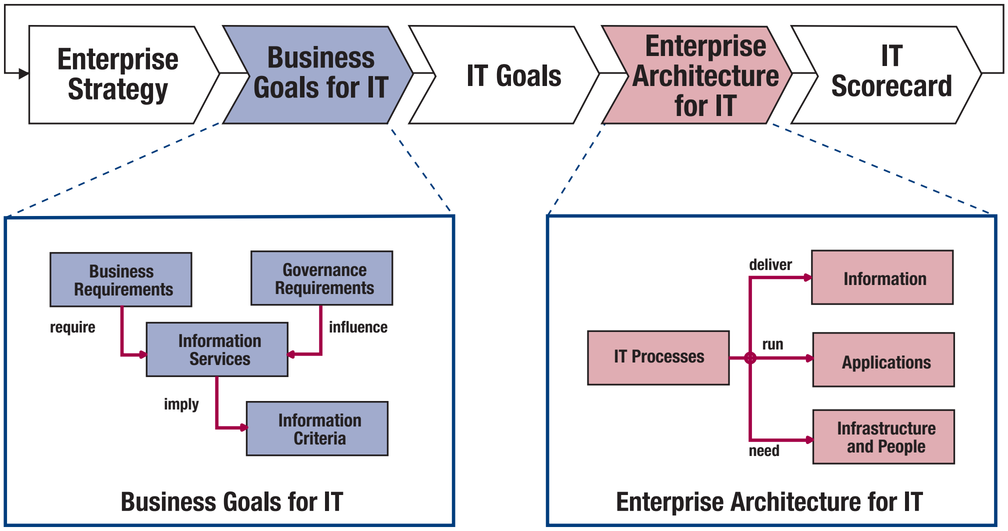
BUSINESS GOALS AND IT GOALS

Whilst information criteria provide a generic method for defining the business requirements, defining a set of generic business and IT goals provides a business-related and 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. Appendix I provides a matrix of generic business goals and IT goals and shows how they map to the information criteria. These generic examples can be used as a guide to determine the specific business requirements, goals and metrics for the enterprise.

If IT is to successfully deliver services to support the enterprise's strategy, there should be a clear ownership and direction of the requirements by the business (the customer) and a clear understanding of what needs to be delivered, and how, by IT (the provider).

Figure 6 illustrates how the enterprise strategy should be translated by the business into objectives related to IT-enabled initiatives (the business goals for IT). These objectives should lead to a clear definition of IT's own objectives (the IT goals), which in turn define the IT resources and capabilities (the enterprise architecture for IT) required to successfully execute IT's part of the enterprise's strategy.[1] Once the aligned goals have been defined, they need to be monitored to ensure that actual delivery matches expectations. This is achieved by metrics that are derived from the goals and captured in an IT scorecard.

Figure 6—Defining IT Goals and Enterprise Architecture for IT



For the customer to understand the IT goals and IT scorecard, all of these objectives and associated metrics should be expressed in business terms meaningful to the customer. This, combined with an effective alignment of the hierarchy of objectives, will ensure that the business can confirm that IT is likely to support the enterprise's goals.

[1] It needs to be noted that the definition and implementation of an enterprise architecture for IT will also create internal IT goals that contribute to, but are not directly derived from, the business goals.

Appendix I, Tables Linking Goals and Processes, provides a global view of how generic business goals relate to IT goals, IT processes and information criteria. The tables help demonstrate the scope of COBIT and the overall business relationship between COBIT and enterprise drivers. As **figure 6** illustrates, these drivers come from the business and from the governance layer of the enterprise, the former focusing more on functionality and speed of delivery, the latter more on cost-efficiency, return on investment (ROI) and compliance.

IT RESOURCES

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 while leveraging business information. These resources, together with the processes, constitute an enterprise architecture for IT, as shown in **figure 6**.

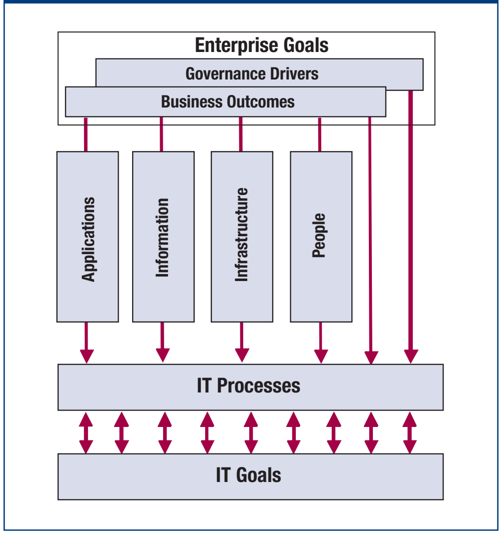
To respond to the business requirements for IT, the enterprise needs to invest in the resources required to create an adequate technical capability (e.g., an enterprise resource planning [ERP] system) to support a business capability (e.g., implementing a supply chain) resulting in the desired outcome (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 (i.e., hardware, operating systems, database management systems, networking, multimedia, 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.

Figure 7 summarises how the business goals for IT influence how the IT resources need to be managed by the IT processes to deliver IT's goals.

Figure 7—Managing IT Resources to Deliver IT Goals



Process-oriented

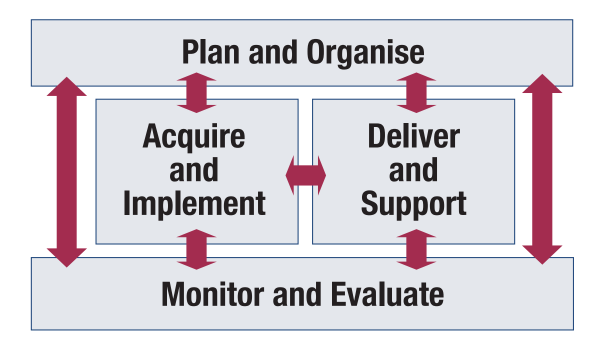
COBIT defines IT activities in a generic process model within four domains. These domains are Plan and Organise, Acquire and Implement, Deliver and Support, and Monitor and Evaluate. The domains map to IT's traditional responsibility areas of plan, build, run and monitor.

The COBIT framework provides a reference process model and common language for everyone in an enterprise to view and manage IT activities. Incorporating an operational model and a common language for all parts of the business involved in IT is one of the most important and initial steps toward good governance. It also provides a framework for measuring and monitoring IT performance, communicating with service providers and integrating best management practices. 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. They are usually ordered into the responsibility domains of plan, build, run and monitor. Within the COBIT framework, these domains, as shown in **figure 8**, are called:

- **Plan and Organise (PO)**—Provides direction to solution delivery (AI) and service delivery (DS)
- **Acquire and Implement (AI)**—Provides the solutions and passes them to be turned into services
- **Deliver and Support (DS)**—Receives the solutions and makes them usable for end users
- **Monitor and Evaluate (ME)**—Monitors all processes to ensure that the direction provided is followed

Figure 8—The Four Interrelated Domains of COBIT



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 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 for information security?

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 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 adequate confidentiality, integrity and availability controls in place for information security?

Across these four domains, COBIT has identified 34 IT processes that are generally used (refer to **figure 22** for the complete list). While most enterprises have defined plan, build, run and monitor responsibilities for IT, and most have the same key processes, few will have the same process structure or apply all 34 COBIT processes. COBIT provides a complete list of processes that can be used to verify the completeness of activities and responsibilities; however, they need not all apply, and, even more, they can be combined as required by each enterprise.

For each of these 34 processes, a link is made to the business and IT goals that are supported. Information on how the goals can be measured, what the key activities and major deliverables are, and who is responsible for them is also provided.

Controls-based

COBIT defines control objectives for all 34 processes, as well as overarching process and application controls.

PROCESSES NEED 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. They:

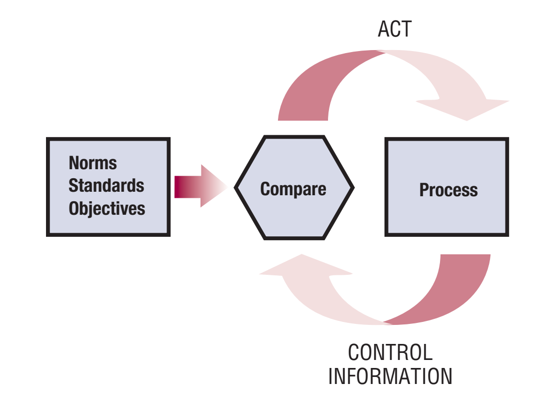
- Are statements of managerial actions to increase value or reduce risk
- Consist of policies, procedures, practices and organisational structures
- Are designed to provide reasonable assurance that business objectives will be achieved and undesired events will be prevented or detected and corrected

Enterprise management needs to make choices relative to these control objectives by:

- Selecting those that are applicable
- Deciding upon those that will be implemented
- Choosing how to implement them (frequency, span, automation, etc.)
- Accepting the risk of not implementing those that may apply

Guidance can be obtained from the standard control model shown in **figure 9**. It follows the principles evident in this analogy: When the room temperature (standard) for the heating system (process) is set, the system will constantly check (compare) ambient room temperature (control information) and will signal (act) the heating system to provide more or less heat.

Figure 9—Control Model



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, 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.

The control objectives are identified by a two-character domain reference (PO, AI, DS and ME) plus a process number and a control objective number. In addition to the control objectives, each COBIT process has generic control requirements that are identified by PCn, for process control number. They should be considered together with the process control objectives to have a complete view of control requirements.

PC1 Process Goals and Objectives

Define and communicate specific, measurable, actionable, realistic, results-oriented and timely (SMARRT) process goals and objectives for the effective execution of each IT process. Ensure that they are linked to the business goals and supported by suitable metrics.

PC2 Process Ownership

Assign an owner for each IT process, and clearly define the roles and responsibilities of the process owner. Include, for example, responsibility for process design, interaction with other processes, accountability for the end results, measurement of process performance and the identification of improvement opportunities.

PC3 Process Repeatability

Design and establish each key IT process such that it is repeatable and consistently produces the expected results. Provide for a logical but flexible and scaleable sequence of activities that will lead to the desired results and is agile enough to deal with exceptions and emergencies. Use consistent processes, where possible, and tailor only when unavoidable.

PC4 Roles and Responsibilities

Define the key activities and end deliverables of the process. Assign and communicate unambiguous roles and responsibilities for effective and efficient execution of the key activities and their documentation as well as accountability for the process end deliverables.

PC5 Policy, Plans and Procedures

Define and communicate how all policies, plans and procedures that drive an IT process are documented, reviewed, maintained, approved, stored, communicated and used for training. Assign responsibilities for each of these activities and, at appropriate times, review whether they are executed correctly. Ensure that the policies, plans and procedures are accessible, correct, understood and up to date.

PC6 Process Performance Improvement
Identify a set of metrics that provides insight into the outcomes and performance of the process. Establish targets that reflect on the process goals and performance indicators that enable the achievement of process goals. Define how the data are to be obtained. Compare actual measurements to targets and take action upon deviations, where necessary. Align metrics, targets and methods with IT's overall performance monitoring approach.

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.

In addition, COBIT provides examples for each process that are illustrative, but not prescriptive or exhaustive, of:
- Generic inputs and outputs
- Activities and guidance on roles and responsibilities in a Responsible, Accountable, Consulted and Informed (RACI) chart
- Key activity goals (the most important things to do)
- Metrics

In addition to appreciating what controls are required, process owners need to understand what inputs they require from others and what others require from their process. COBIT provides generic examples of the key inputs and outputs for each process, including external IT requirements. There are some outputs that are input to all other processes, marked as 'ALL' in the output tables, but they are not mentioned as inputs in all processes, and typically include quality standards and metrics requirements, the IT process framework, documented roles and responsibilities, the enterprise IT control framework, IT policies, and personnel roles and responsibilities.

Understanding the roles and responsibilities for each process is key to effective governance. COBIT provides a RACI chart for each process. Accountable means 'the buck stops here'—this is the person who provides direction and authorises an activity. Responsibility is attributed to the person who gets the task done. The other two roles (consulted and informed) ensure that everyone who needs to be is involved and supports the process.

BUSINESS AND IT CONTROLS

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.

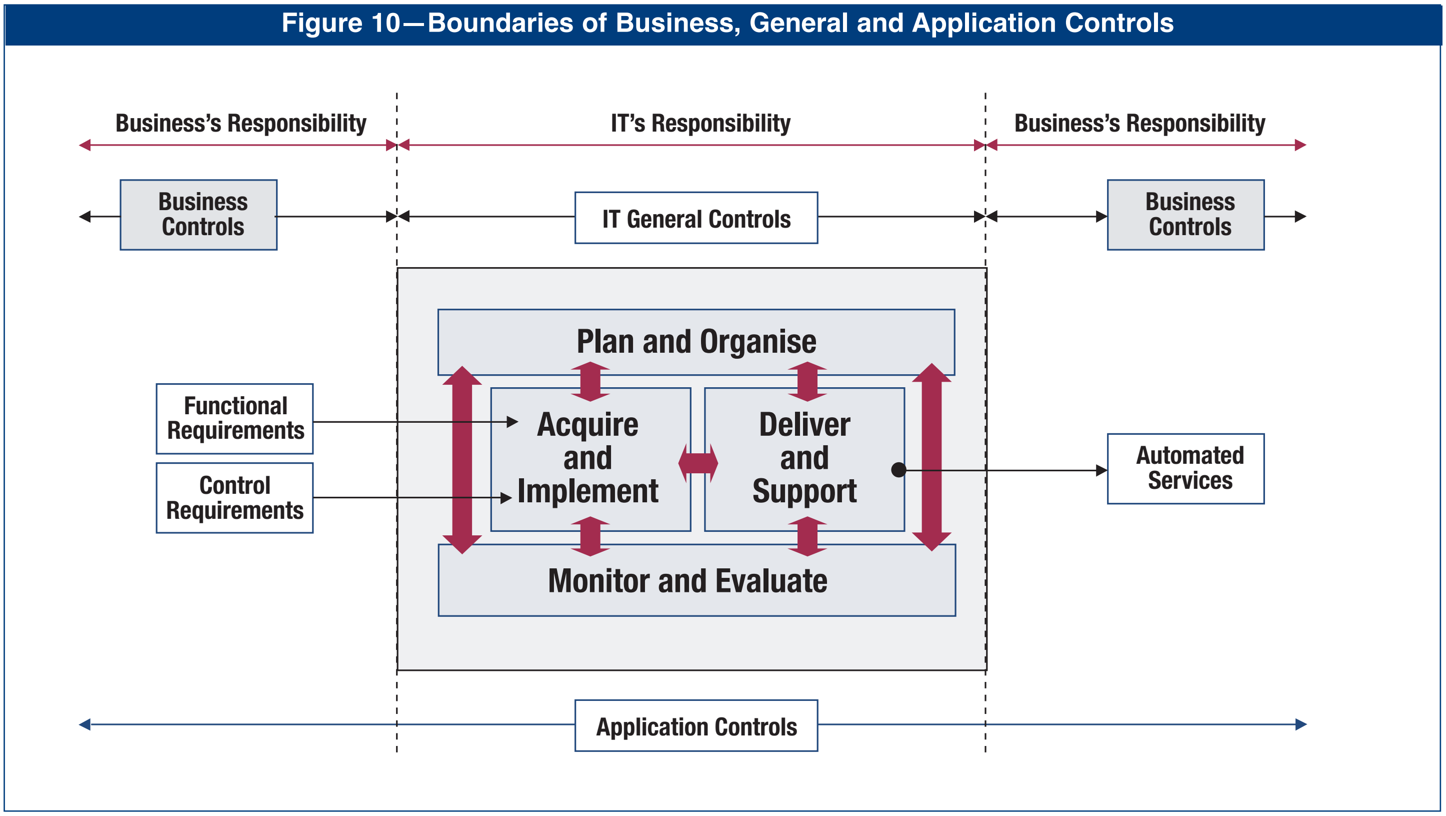
IT GENERAL CONTROLS AND APPLICATION CONTROLS

General controls are controls embedded in IT processes and services. Examples include:
- Systems development
- Change management
- Security
- Computer operations

Controls embedded in business process applications are commonly referred to as application controls. Examples include:
- Completeness
- Accuracy
- Validity
- Authorisation
- Segregation of duties

COBIT assumes the design and implementation of automated application controls to be the responsibility of IT, covered in the Acquire and Implement domain, based on business requirements defined using COBIT's information criteria, as shown in **figure 10**. The operational management and control responsibility for application controls is not with IT, but with the business process owner.

Figure 10—Boundaries of Business, General and Application Controls



Hence, the responsibility for application controls is an end-to-end joint responsibility between business and IT, but the nature of the responsibilities changes as follows:

- The business is responsible to properly:
  - Define functional and control requirements
  - Use automated services
- IT is responsible to:
  - Automate and implement business functional and control requirements
  - 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. They are identified by ACn, for application control number.

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. Detect errors and irregularities 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. Correction and resubmission of data that were erroneously input should be performed without compromising original transaction authorisation levels. Where appropriate for reconstruction, retain original source documents for the appropriate amount of time.

AC3 Accuracy, Completeness and Authenticity Checks
Ensure that transactions are accurate, complete and valid. Validate data that were input, and edit or send back for correction 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 does not disrupt the processing of valid transactions.

AC5 Output Review, Reconciliation and Error Handling
Establish procedures and associated responsibilities to ensure that output is handled in an authorised manner, delivered to the appropriate recipient, and protected during transmission; that verification, detection and correction of the accuracy of output occurs; and that information provided in the output is used.

AC6 Transaction Authentication and Integrity
Before passing transaction data between internal applications and business/operational functions (in or outside the enterprise), check it 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 itself: 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. What should be measured and how? Enterprises need to measure where they are and where improvement is required, and implement a management tool kit to monitor this improvement. COBIT deals with these issues by providing:

- Maturity models to enable benchmarking and identification of necessary capability improvements
- Performance goals and metrics for the IT processes, demonstrating how processes meet business and IT goals and are used for measuring internal process performance based on balanced scorecard principles
- Activity goals for enabling effective process performance

MATURITY MODELS

Senior managers in corporate and public enterprises are increasingly asked to consider how well IT is being managed. In response to this, business cases require development for improvement and reaching the appropriate level of management and control over the information infrastructure. While few would argue that this is not a good thing, they need to consider the cost-benefit balance and these related questions:

- What are our industry peers doing, and how are we placed in relation to them?
- What is acceptable industry good practice, and how are we placed with regard to these practices?
- Based upon these comparisons, can we be said to be doing enough?
- How do we identify what is required to be done to reach an adequate level of management and control over our IT processes?

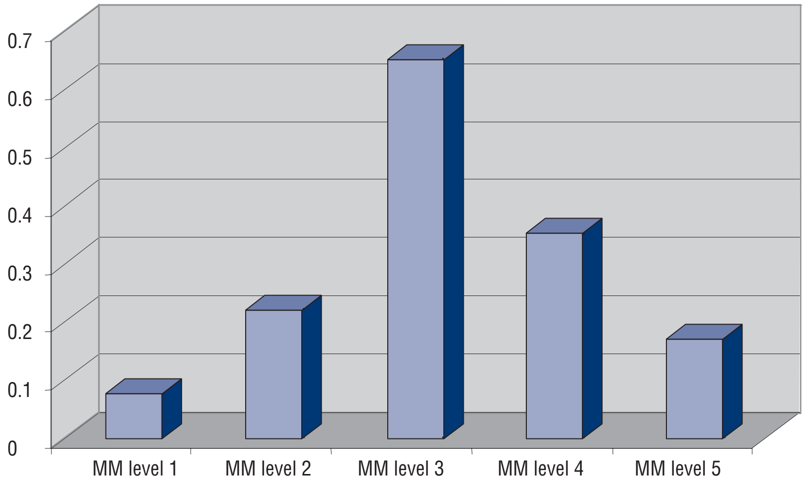
It can be difficult to supply meaningful answers to these questions. IT management is constantly on the lookout for benchmarking and self-assessment tools in response to the need to know what to do in an efficient manner. Starting from COBIT's processes, the process owner should be able to incrementally benchmark against that control objective. This responds to three needs:

1. A relative measure of where the enterprise is
2. A manner to efficiently decide where to go
3. A tool for measuring progress against the goal

Maturity modelling for management and control over IT processes is based on a method of evaluating the organisation, so it can be rated from a maturity level of non-existent (0) to optimised (5). This approach is derived from the maturity model that the Software Engineering Institute (SEI) defined for the maturity of software development capability. Although concepts of the SEI approach were followed, the COBIT implementation differs considerably from the original SEI, which was oriented toward software product engineering principles, organisations striving for excellence in these areas and formal appraisal of maturity levels so that software developers could be 'certified'. In COBIT, a generic definition is provided for the COBIT maturity scale, which is similar to CMM but interpreted for the nature of COBIT's IT management processes. A specific model is provided from this generic scale for each of COBIT's 34 processes. Whatever the model, the scales should not be too granular, as that would render the system difficult to use and suggest a precision that is not justifiable because, in general, the purpose is to identify where issues are and how to set priorities for improvements. The purpose is not to assess the level of adherence to the control objectives.

The maturity levels are designed as profiles of IT processes that an enterprise would recognise as descriptions of possible current and future states. They are not designed for use as a threshold model, where one cannot move to the next higher level without having fulfilled all conditions of the lower level. With COBIT's maturity models, unlike the original SEI CMM approach, there is no intention to measure levels precisely or try to certify that a level has exactly been met. A COBIT maturity assessment is likely to result in a profile where conditions relevant to several maturity levels will be met, as shown in the example graph in **figure 11**.

Figure 11—Possible Maturity Level of an IT Process



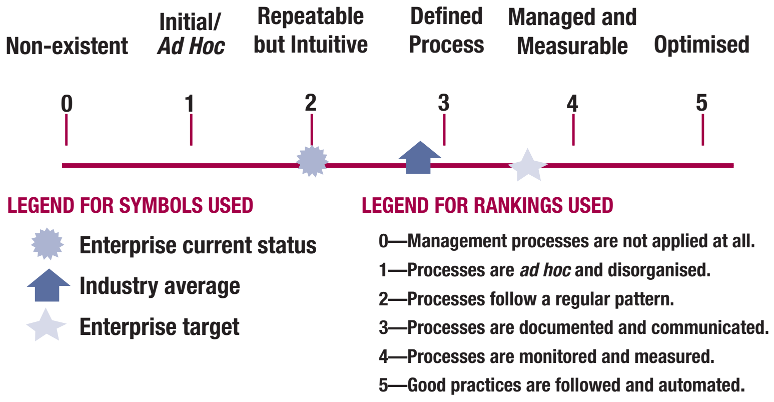
Possible maturity level of an IT process: The example illustrates a process that is largely at level 3 but still has some compliance issues with lower level requirements whilst already investing in performance measurement (level 4) and optimisation (level 5)

This is because when assessing maturity using COBIT's models, it will often be the case that some implementation will be in place at different levels even if it is not complete or sufficient. These strengths can be built on to further improve maturity. For example, some parts of the process can be well defined, and, even if it is incomplete, it would be misleading to say the process is not defined at all.

Using the maturity models developed for each of COBIT's 34 IT processes, management can identify:
- The actual performance of the enterprise—Where the enterprise is today
- The current status of the industry—The comparison
- The enterprise's target for improvement—Where the enterprise wants to be
- The required growth path between 'as-is' and 'to-be'

To make the results easily usable in management briefings, where they will be presented as a means to support the business case for future plans, a graphical presentation method needs to be provided (**figure 12**).

Figure 12—Graphic Representation of Maturity Models



0—Management processes are not applied at all.
1—Processes are *ad hoc* and disorganised.
2—Processes follow a regular pattern.
3—Processes are documented and communicated.
4—Processes are monitored and measured.
5—Good practices are followed and automated.

The development of the graphical representation was based on the generic maturity model descriptions shown in **figure 13**.

Figure 13—Generic Maturity Model

0 Non-existent—Complete lack of any recognisable processes. The enterprise has not even recognised that there is an issue to be addressed.

1 Initial/*Ad Hoc*—There is evidence that the enterprise has recognised that the issues exist and need to be addressed. There are, however, no standardised processes; instead, there are *ad hoc* approaches that tend to be applied on an individual or case-by-case basis. The overall approach to management is disorganised.

2 Repeatable but Intuitive—Processes have developed to the stage where similar procedures are followed by different people undertaking the same task. There is no formal training or communication of standard procedures, and responsibility is left to the individual. There is a high degree of reliance on the knowledge of individuals and, therefore, errors are likely.

3 Defined Process—Procedures have been standardised and documented, and communicated through training. It is mandated that these processes should be followed; however, it is unlikely that deviations will be detected. The procedures themselves are not sophisticated but are the formalisation of existing practices.

4 Managed and Measurable—Management monitors and measures compliance with procedures and takes action where processes appear not to be working effectively. Processes are under constant improvement and provide good practice. Automation and tools are used in a limited or fragmented way.

5 Optimised—Processes have been refined to a level of good practice, based on the results of continuous improvement and maturity modelling with other enterprises. IT is used in an integrated way to automate the workflow, providing tools to improve quality and effectiveness, making the enterprise quick to adapt.

COBIT is a framework developed for IT process management with a strong focus on control. These scales need to be practical to apply and reasonably easy to understand. The topic of IT process management is inherently complex and subjective and, therefore, is best approached through facilitated assessments that raise awareness, capture broad consensus and motivate improvement. These assessments can be performed either against the maturity level descriptions as a whole or with more rigour against each of the individual statements of the descriptions. Either way, expertise in the enterprise's process under review is required.

The advantage of a maturity model approach is that it is relatively easy for management to place itself on the scale and appreciate what is involved if improved performance is needed. The scale includes 0 because it is quite possible that no process exists at all. The 0-5 scale is based on a simple maturity scale showing how a process evolves from a non-existent capability to an optimised capability.

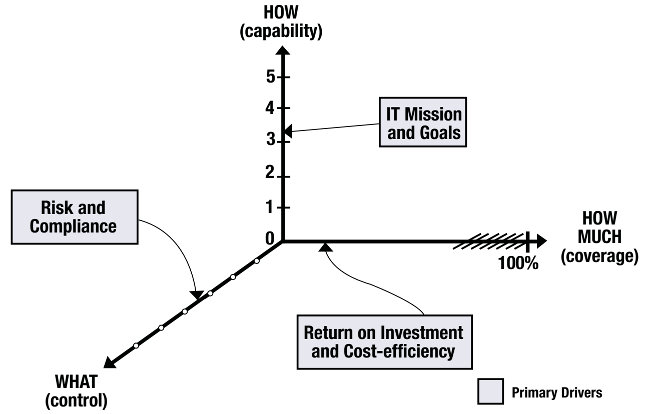
However, process management capability is not the same as process performance. The required capability, as determined by business and IT goals, may not need to be applied to the same level across the entire IT environment, e.g., not consistently or to only a limited number of systems or units. Performance measurement, as covered in the next paragraphs, is essential in determining what the enterprise's actual performance is for its IT processes.

Although a properly applied capability already reduces risks, an enterprise still needs to analyse the controls necessary to ensure that risk is mitigated and value is obtained in line with the risk appetite and business objectives. These controls are guided by COBIT's control objectives. Appendix III provides a maturity model on internal control that illustrates the maturity of an enterprise relative to establishment and performance of internal control. Often this analysis is initiated in response to external drivers, but ideally it should be instituted as documented by COBIT processes PO6 *Communicate management aims and directions* and ME2 *Monitor and evaluate internal control.*

Capability, coverage and control are all dimensions of process maturity, as illustrated in **figure 14**.

The maturity model is a way of measuring how well developed management processes are, i.e., how capable they actually are. How well developed or capable they should be primarily depends on the IT goals and the underlying business needs they support. How much of that capability is actually deployed largely depends on the return an enterprise wants from the investment. For example, there will be critical processes and systems that need more and tighter security management than others that are less critical. On the other hand, the degree and sophistication of controls that need to be applied in a process are more driven by the enterprise's risk appetite and applicable compliance requirements.

Figure 14—The Three Dimensions of Maturity



The maturity model scales will help professionals explain to managers where IT process management shortcomings exist and set targets for where they need to be. The right maturity level will be influenced by the enterprise's business objectives, the operating environment and industry practices. Specifically, the level of management maturity will depend on the enterprise's dependence on IT, its technology sophistication and, most important, the value of its information.
A strategic reference point for an enterprise to improve management and control of IT processes can be found by looking at emerging international standards and best-in-class practices. The emerging practices of today may become the expected level of performance of tomorrow and, therefore, are useful for planning where an enterprise wants to be over time.

The maturity models are built up starting from the generic qualitative model (see **figure 13**) to which principles from the following attributes are added in an increasing manner through the levels:

- Awareness and communication
- Policies, plans and procedures
- Tools and automation
- Skills and expertise
- Responsibility and accountability
- Goal setting and measurement

The maturity attribute table shown in **figure 15** lists the characteristics of how IT processes are managed and describes how they evolve from a non-existent to an optimised process. These attributes can be used for more comprehensive assessment, gap analysis and improvement planning.

In summary, maturity models provide a generic profile of the stages through which enterprises evolve for management and control of IT processes. They are:

- A set of requirements and the enabling aspects at the different maturity levels
- A scale where the difference can be made measurable in an easy manner
- A scale that lends itself to pragmatic comparison
- The basis for setting as-is and to-be positions
- Support for gap analysis to determine what needs to be done to achieve a chosen level
- Taken together, a view of how IT is managed in the enterprise

The COBIT maturity models focus on maturity, but not necessarily on coverage and depth of control. They are not a number for which to strive, nor are they designed to be a formal basis for certification with discrete levels that create thresholds that are difficult to cross. However, they are designed to be always applicable, with levels that provide a description an enterprise can recognise as best fitting its processes. The right level is determined by the enterprise type, environment and strategy.

Coverage, depth of control, and how the capability is used and deployed are cost-benefit decisions. For example, a high level of security management may have to be focused only on the most critical enterprise systems. Another example would be the choice between a weekly manual review and a continuous automated control.

Finally, whilst higher levels of maturity increase control over the process, the enterprise still needs to analyse, based on risk and value drivers, which control mechanisms it should apply. The generic business and IT goals defined in this framework will help with this analysis. The control mechanisms are guided by COBIT's control objectives and focus on what is done in the process; the maturity models primarily focus on how well a process is managed. Appendix III provides a generic maturity model showing the status of the internal control environment and the establishment of internal controls in an enterprise.

A properly implemented control environment is attained when all three aspects of maturity (capability, coverage and control) have been addressed. Improving maturity reduces risk and improves efficiency, leading to fewer errors, more predictable processes and a cost-efficient use of resources.

PERFORMANCE MEASUREMENT

Goals and metrics are defined in COBIT at three levels:

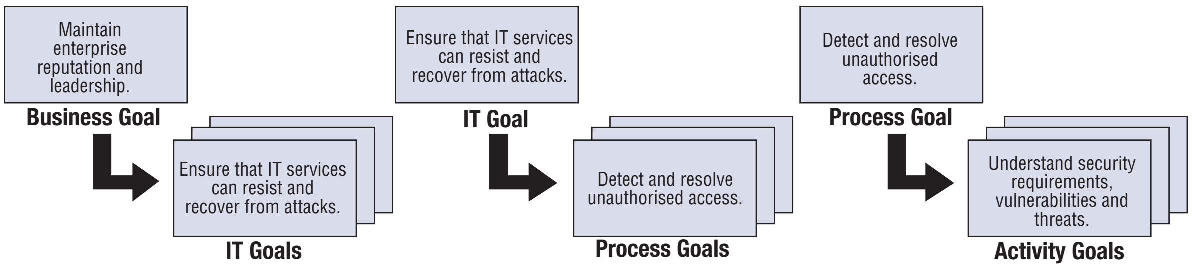
- IT goals and metrics that define what the business expects from IT and how to measure it
- Process goals and metrics that define what the IT process must deliver to support IT's objectives and how to measure it
- Activity goals and metrics that establish what needs to happen inside the process to achieve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

Figure 15—Maturity Attribute Table

	Awareness and Communication	Policies, Plans and Procedures	Tools and Automation	Skills and Expertise	Responsibility and Accountability	Goal Setting and Measurement
1	Recognition of the need for the process is emerging. There is sporadic communication of the issues.	There are *ad hoc* approaches to processes and practices. The process and policies are undefined.	Some tools may exist; usage is based on standard desktop tools. There is no planned approach to the tool usage.	Skills required for the process are not identified. A training plan does not exist and no formal training occurs.	There is no definition of accountability and responsibility. People take ownership of issues based on their own initiative on a reactive basis.	Goals are not clear and no measurement takes place.
2	There is awareness of the need to act. Management communicates the overall issues.	Similar and common processes emerge, but are largely intuitive because of individual expertise. Some aspects of the process are repeatable because of individual expertise, and some documentation and informal understanding of policy and procedures may exist.	Common approaches to use of tools exist but are based on solutions developed by key individuals. Vendor tools may have been acquired, but are probably not applied correctly, and may even be shelfware.	Minimum skill requirements are identified for critical areas. Training is provided in response to needs, rather than on the basis of an agreed plan, and informal training on the job occurs.	An individual assumes his/her responsibility and is usually held accountable, even if this is not formally agreed. There is confusion about responsibility when problems occur, and a culture of blame tends to exist.	Some goal setting occurs; some financial measures are established but are known only by senior management. There is inconsistent monitoring in isolated areas.
3	There is understanding of the need to act. Management is more formal and structured in its communication.	Usage of good practices emerges. The process, policies and procedures are defined and documented for all key activities.	A plan has been defined for use and standardisation of tools to automate the process. Tools are being used for their basic purposes, but may not all be in accordance with the agreed plan, and may not be integrated with one another.	Skill requirements are defined and documented for all areas. A formal training plan has been developed, but formal training is still based on individual initiatives.	Process responsibility and accountability are defined and process owners have been identified. The process owner is unlikely to have the full authority to exercise the responsibilities.	Some effectiveness goals and measures are set, but are not communicated, and there is a clear link to business goals. Measurement processes emerge, but are not consistently applied. IT balanced scorecard ideas are being adopted, as is occasional intuitive application of root cause analysis.
4	There is understanding of the full requirements. Mature communication techniques are applied and standard communication tools are in use.	The process is sound and complete; internal best practices are applied. All aspects of the process are documented and repeatable. Policies have been approved and signed off on by management. Standards for developing and maintaining the processes and procedures are adopted and followed.	Tools are implemented according to a standardised plan, and some have been integrated with other related tools. Tools are being used in main areas to automate management of the process and monitor critical activities and controls.	Skill requirements are routinely updated for all areas, proficiency is ensured for all critical areas, and certification is encouraged. Mature training techniques are applied according to the training plan, and knowledge sharing is encouraged. All internal domain experts are involved, and the effectiveness of the training plan is assessed.	Process responsibility and accountability are accepted and working in a way that enables a process owner to fully discharge his/her responsibilities. A reward culture is in place that motivates positive action.	Efficiency and effectiveness are measured and communicated and linked to business goals and the IT strategic plan. The IT balanced scorecard is implemented in some areas with exceptions noted by management and root cause analysis is being standardised. Continuous improvement is emerging.
5	There is advanced, forward-looking understanding of requirements. Proactive communication of issues based on trends exists, mature communication techniques are applied, and integrated communication tools are in use.	External best practices and standards are applied. Process documentation is evolved to automated workflows. Processes, policies and procedures are standardised and integrated to enable end-to-end management and improvement.	Standardised tool sets are used across the enterprise. Tools are fully integrated with other related tools to enable end-to-end support of the processes. Tools are being used to support improvement of the process and automatically detect control exceptions.	The organisation formally encourages continuous improvement of skills, based on clearly defined personal and organisational goals. Training and education support external best practices and use of leading-edge concepts and techniques. Knowledge sharing is an enterprise culture, and knowledge-based systems are being deployed. External experts and industry leaders are used for guidance.	Process owners are empowered to make decisions and take action. The acceptance of responsibility has been cascaded down throughout the organisation in a consistent fashion.	There is an integrated performance measurement system linking IT performance to business goals by global application of the IT balanced scorecard. Exceptions are globally and consistently noted by management and root cause analysis is applied. Continuous improvement is a way of life.

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. **Figure 16** provides examples of the business, IT, process and activity goal relationship.

Figure 16—Example of Goal Relationships

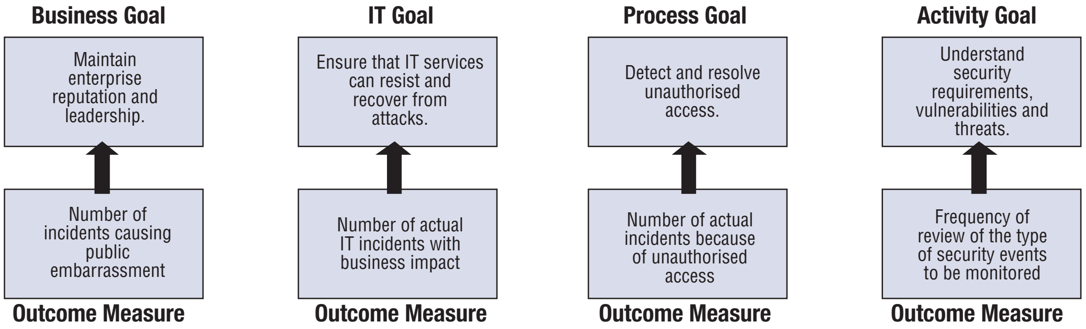

Maintain enterprise reputation and leadership.
Business Goal
Ensure that IT services can resist and recover from attacks.
IT Goals
Ensure that IT services can resist and recover from attacks.
IT Goal
Detect and resolve unauthorised access.
Process Goals
Detect and resolve unauthorised access.
Process Goal
Understand security requirements, vulnerabilities and threats.
Activity Goals

The terms KGI and KPI, used in previous versions of COBIT, have been replaced with 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'.

Figure 17 provides possible goal or outcome measures for the example used.

Figure 17—Possible Outcome Measures for the Example in Figure 16

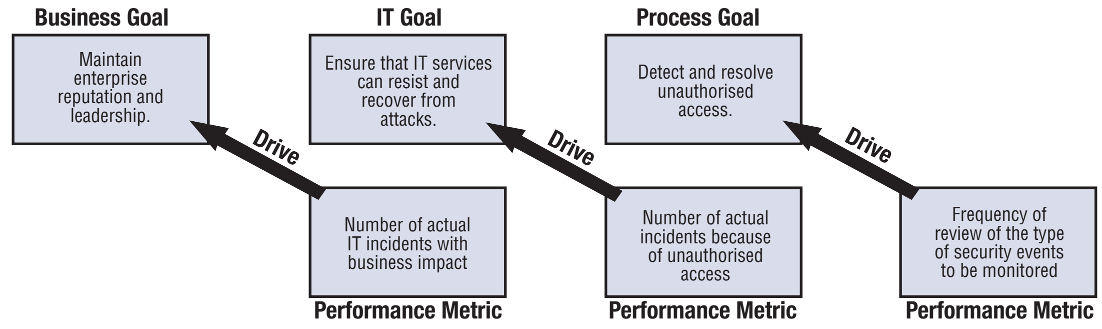

Business Goal
Maintain enterprise reputation and leadership.
Number of incidents causing public embarrassment
Outcome Measure
IT Goal
Ensure that IT services can resist and recover from attacks.
Number of actual IT incidents with business impact
Outcome Measure
Process Goal
Detect and resolve unauthorised access.
Number of actual incidents because of unauthorised access
Outcome Measure
Activity Goal
Understand security requirements, vulnerabilities and threats.
Frequency of review of the type of security events to be monitored
Outcome Measure

The outome measures of the lower level become performance indicators for the higher level. As per the example in **figure 16**, an outcome measure indicating that detection and resolution of unauthorised access are on target will also indicate that it will be more likely that IT services can resist and recover from attacks. That is, the outcome measure has become a performance indicator for the higher-level goal. **Figure 18** illustrates how outcome measures for the example become performance metrics.

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

Figure 18—Possible Performance Drivers for the Example in Figure 16

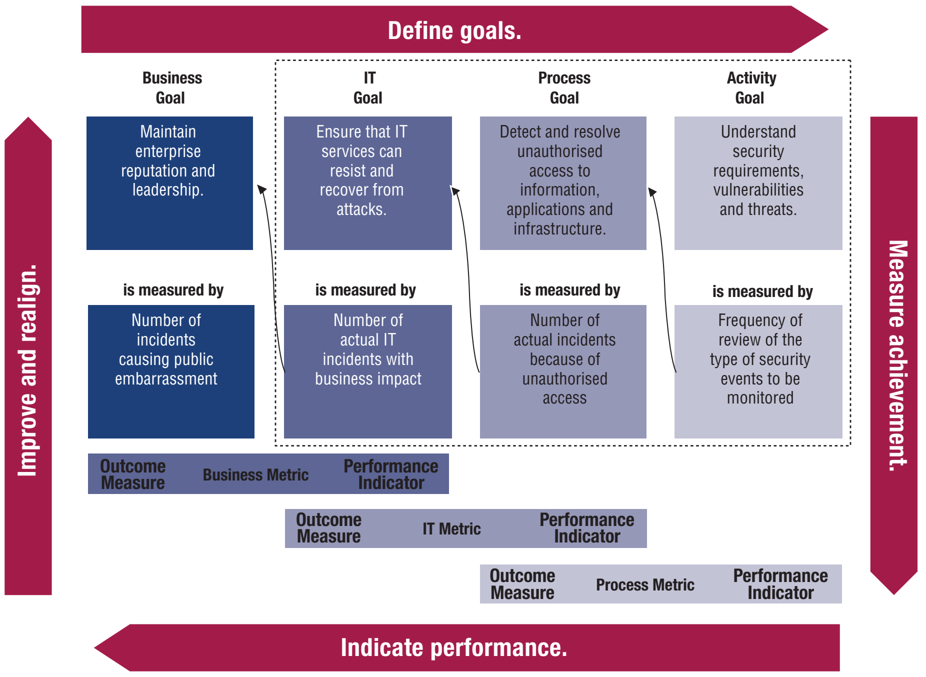

Business Goal
Maintain enterprise reputation and leadership.
IT Goal
Ensure that IT services can resist and recover from attacks.
Process Goal
Detect and resolve unauthorised access.
Drive
Drive
Drive
Number of actual IT incidents with business impact
Number of actual incidents because of unauthorised access
Frequency of review of the type of security events to be monitored
Performance Metric
Performance Metric
Performance Metric

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, as well as a performance indicator driving the higher-level business, IT function or IT process goal.

Figure 19 illustrates the relationship between 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.

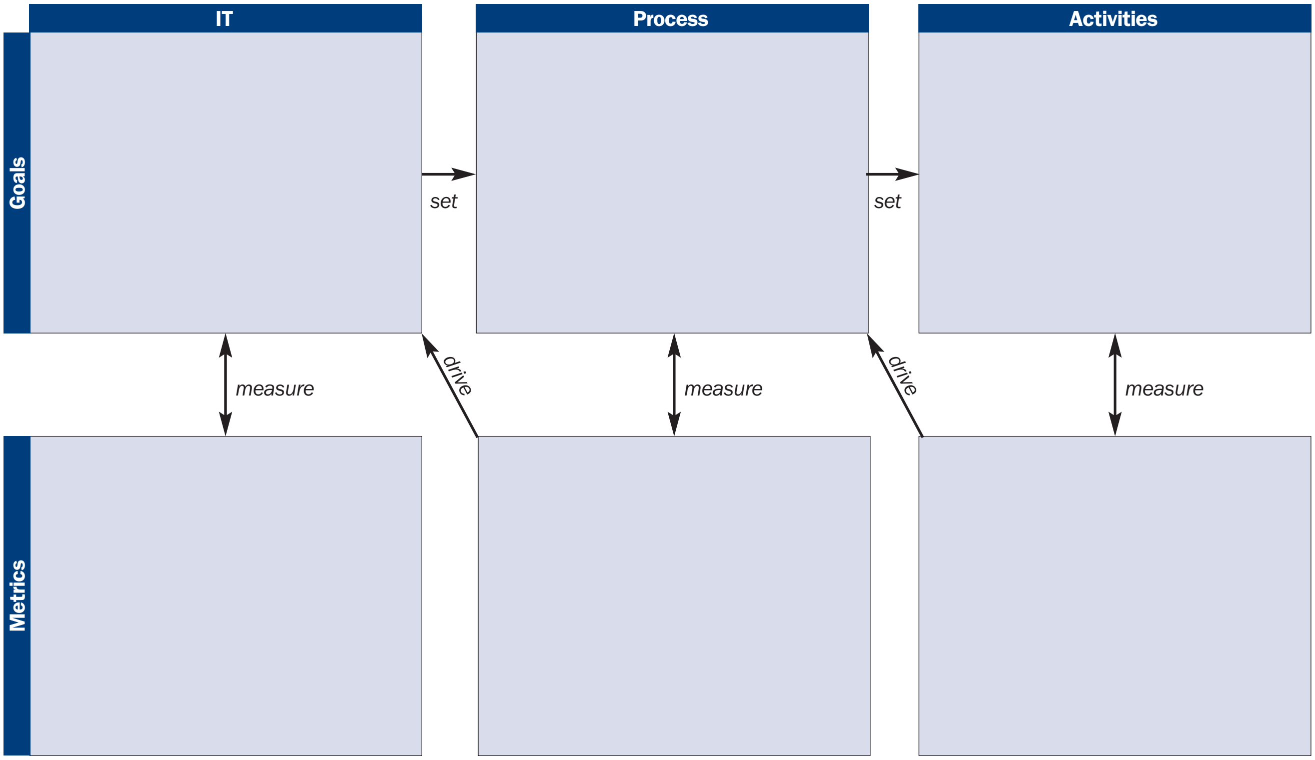
Figure 19—Relationship Amongst Process, Goals and Metrics (DS5)


Define goals.
Business Goal
IT Goal
Process Goal
Activity Goal
Maintain enterprise reputation and leadership.
Ensure that IT services can resist and recover from attacks.
Detect and resolve unauthorised access to information, applications and infrastructure.
Understand security requirements, vulnerabilities and threats.
is measured by
is measured by
is measured by
is measured by
Number of incidents causing public embarrassment
Number of actual IT incidents with business impact
Number of actual incidents because of unauthorised access
Frequency of review of the type of security events to be monitored
Outcome Measure
Business Metric
Performance Indicator
Outcome Measure
IT Metric
Performance Indicator
Outcome Measure
Process Metric
Performance Indicator
Improve and realign.
Measure achievement.
Indicate performance.

The example provided is from DS5 *Ensure systems security*. COBIT provides metrics only up to the IT goals outcome as delineated by the dotted line. While they are also performance indicators for the business goals for IT, COBIT does not provide business goal outcome measures.

The business and IT goals used in the goals and metrics section of COBIT, including their relationship, are provided in appendix I. For each IT process in COBIT, the goals and metrics are presented, as noted in **figure 20**.

Figure 20—Presentation of Goals and Metrics



The metrics have been developed with the following characteristics in mind:

- A high insight-to-effort ratio (i.e., insight into performance and the achievement of goals as compared to the effort to capture them)
- Comparable internally (e.g., percent against a base or numbers over time)
- Comparable externally irrespective of enterprise size or industry
- Better to have a few good metrics (may even be one very good one that could be influenced by different means) than a longer list of lower-quality metrics
- Easy to measure, not to be confused with targets

The COBIT Framework Model

The COBIT framework, therefore, ties the businesses requirements for information and governance to the objectives of the IT services function. The COBIT process model enables IT activities and the resources that support them to be properly managed and controlled based on COBIT's control objectives, and aligned and monitored using COBIT's goals and metrics, as illustrated in **figure 21**.

To summarise, IT resources are managed by IT processes to achieve IT goals that respond to the business requirements. This is the basic principle of the COBIT framework, as illustrated by the COBIT cube (**figure 22**).

Figure 21—COBIT Management, Control, Alignment and Monitoring

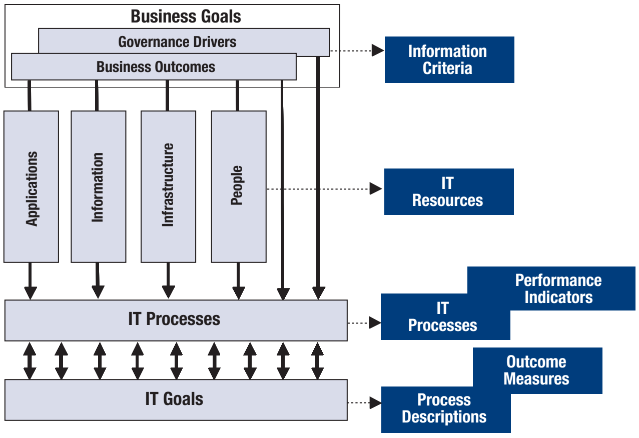
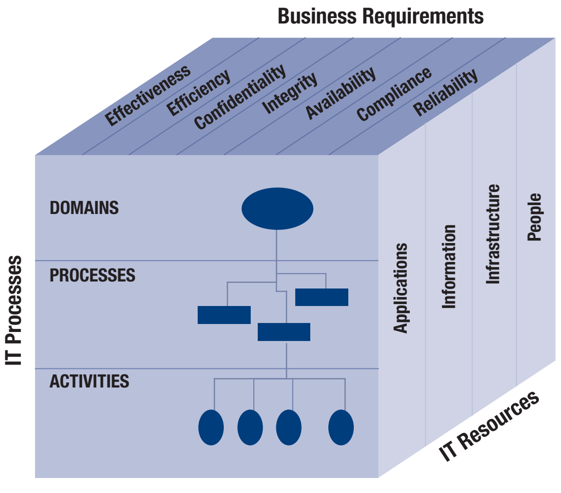


Figure 22—The COBIT Cube



In more detail, the overall COBIT framework can be shown graphically, as depicted in **figure 23**, 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.

COBIT's General Acceptability

COBIT is based on the analysis and harmonisation of existing IT standards and good practices and conforms to generally accepted governance principles. It is positioned at a high level, driven by business requirements, covers the full range of IT activities, and concentrates on *what* should be achieved rather than *how* to achieve effective governance, management and control. Therefore, it acts as an integrator of IT governance practices and appeals to executive management; business and IT management; governance, assurance and security professionals; and IT audit and control professionals. It is designed to be complementary to, and used together with, other standards and good practices.

Implementation of good practices should be consistent with the enterprise's governance and control framework, appropriate for the organisation, and integrated with other methods and practices that are being used. Standards and good practices are not a panacea. Their effectiveness depends on how they have been implemented and kept up to date. They are most useful when applied as a set of principles and as a starting point for tailoring specific procedures. To avoid practices becoming shelfware, management and staff should understand what to do, how to do it and why it is important.

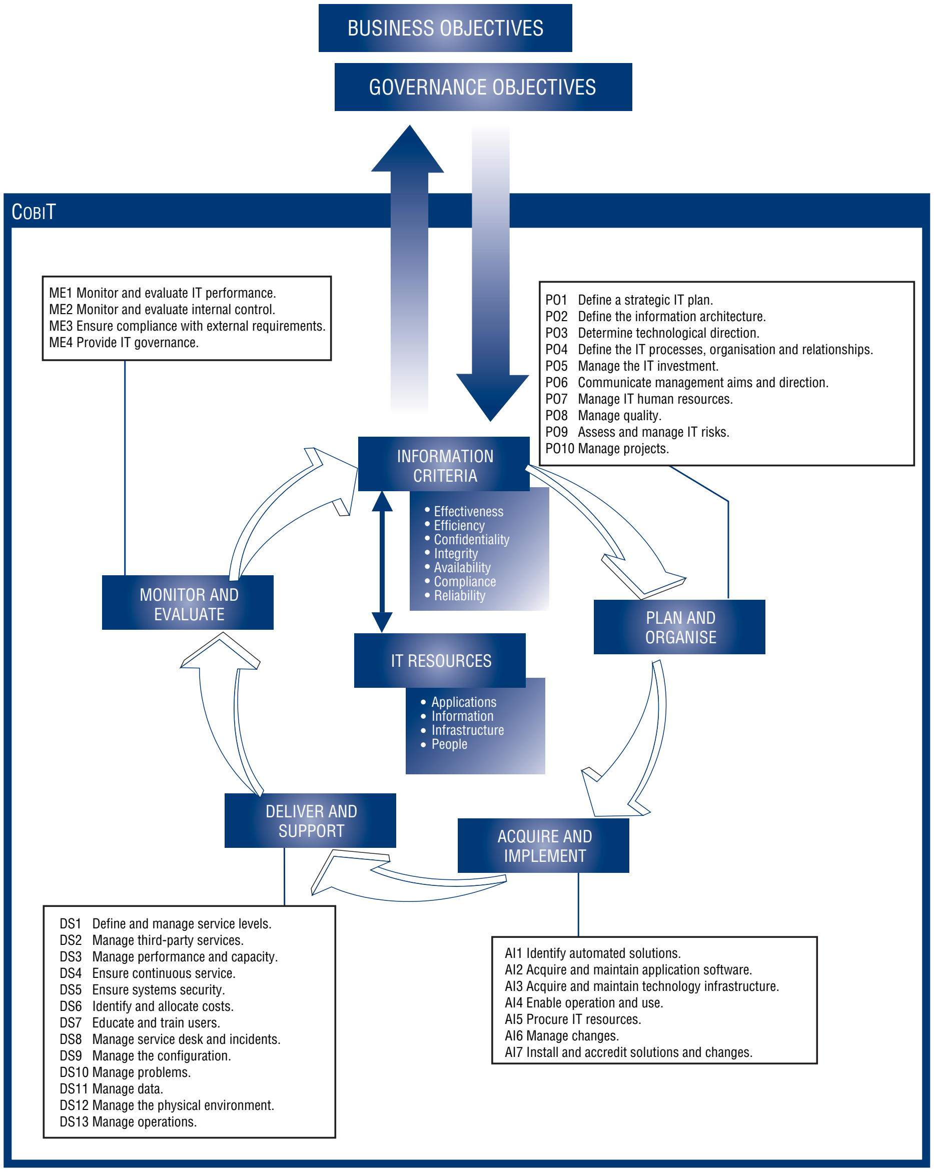
To achieve alignment of good practice to business requirements, it is recommended that COBIT be used at the highest level, providing an overall control framework based on an IT process model that should generically suit every enterprise. Specific practices and standards covering discrete areas can be mapped up to the COBIT framework, thus providing a hierarchy of guidance materials.

COBIT appeals to different users:
- **Executive management**—To obtain value from IT investments and balance risk and control investment in an often unpredictable IT environment
- **Business management**—To obtain assurance on the management and control of IT services provided by internal or third parties
- **IT management**—To provide the IT services that the business requires to support the business strategy in a controlled and managed way
- **Auditors**—To substantiate their opinions and/or provide advice to management on internal controls

COBIT has been developed and is maintained by an independent, not-for-profit research institute, drawing on the expertise of its affiliated association's members, industry experts, and control and security professionals. Its content is based on ongoing research into IT good practice and is continuously maintained, providing an objective and practical resource for all types of users.

COBIT is oriented toward the objectives and scope of IT governance, ensuring that its control framework is comprehensive, in alignment with enterprise governance principles and, therefore, acceptable to boards, executive management, auditors and regulators. In appendix II, a mapping is provided showing how COBIT's control objectives map onto the five focus areas of IT governance and the COSO control activities.

Figure 23—Overall COBIT Framework



ME1 Monitor and evaluate IT performance.
ME2 Monitor and evaluate internal control.
ME3 Ensure compliance with external requirements.
ME4 Provide IT governance.

PO1 Define a strategic IT plan.
PO2 Define the information architecture.
PO3 Determine technological direction.
PO4 Define the IT processes, organisation 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.

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.

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.

Figure 24 summarises how the various elements of the COBIT framework map onto the IT governance focus areas.

Figure 24—COBIT Framework and IT Governance Focus Areas

	Goals	Metrics	Practices	Maturity Models
Strategic alignment	P	P		
Value delivery		P	S	P
Risk management		S	P	S
Resource management		S	P	P
Performance measurement	P	P		S

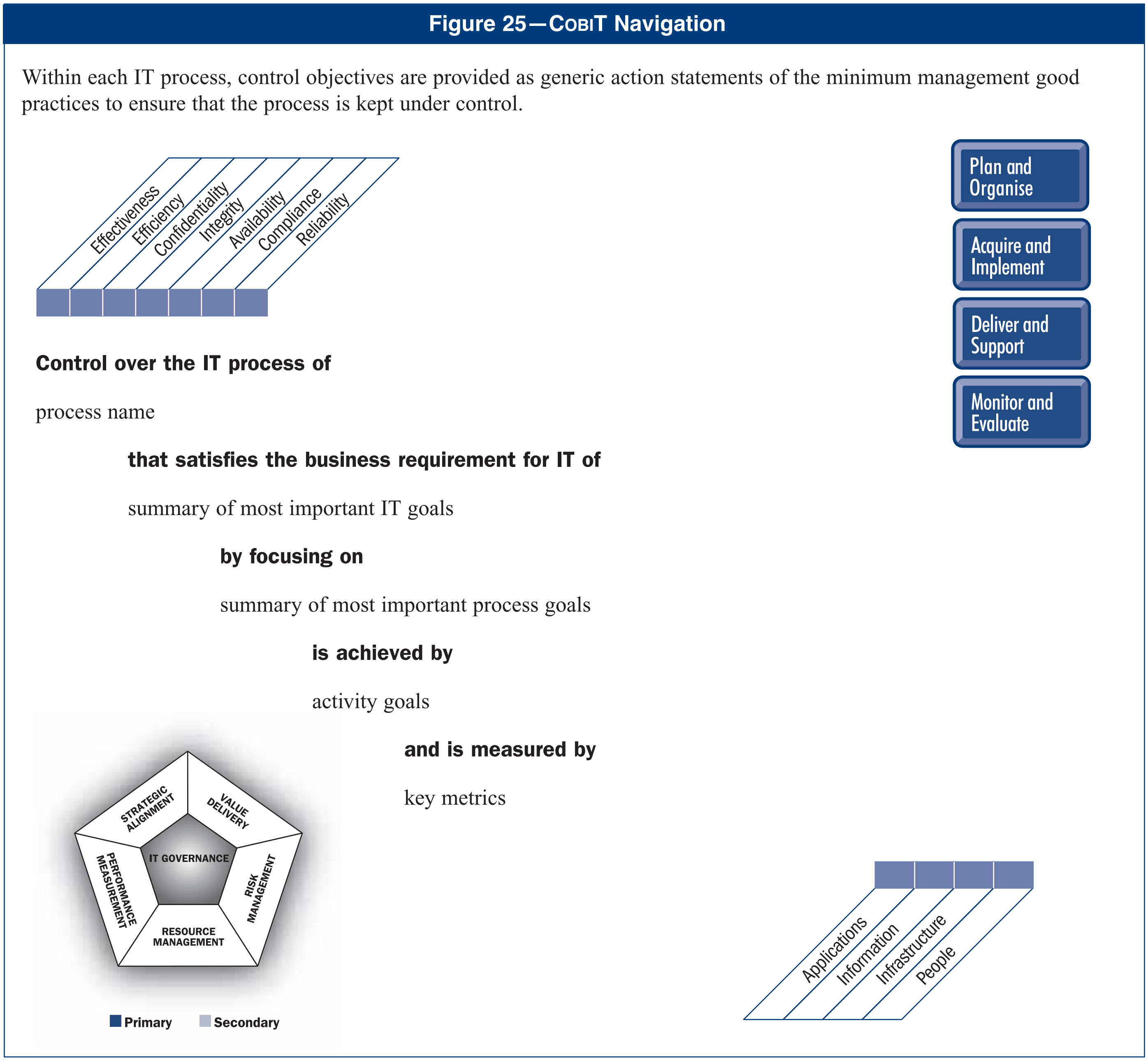
P=Primary enabler S=Secondary enabler

HOW TO USE THIS BOOK

COBIT Framework Navigation

For each of the COBIT IT processes, a description is provided, together with key goals and metrics in the form of a waterfall (**figure 25**).

Figure 25—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.

Control over the IT process of

process name

that satisfies the business requirement for IT of

summary of most important IT goals

by focusing on

summary of most important process goals

is achieved by

activity goals

and is measured by

key metrics

Overview of Core COBIT Components

The COBIT framework is populated with the following core components, provided in the rest of this publication and organised by the 34 IT processes, giving a complete picture of how to control, manage and measure each process. Each process is covered in four sections, and each section constitutes roughly one page, as follows:

- Section 1 (**figure 25**) contains a process description summarising the process objectives, with the process description represented in a waterfall. This page also shows the mapping of the process to the information criteria, IT resources and IT governance focus areas by way of P to indicate primary relationship and S to indicate secondary.

- Section 2 contains the control objectives for this process.
- Section 3 contains the process inputs and outputs, RACI chart, goals and metrics.
- Section 4 contains the maturity model for the process.

Another way of viewing the process performance content is:

- Process inputs are what the process owner needs from others.
- The process description control objectives describe what the process owner needs to do.
- The process outputs are what the process owner has to deliver.
- The goals and metrics show how the process should be measured.
- The RACI chart defines what has to be delegated and to whom.
- The maturity model shows what has to be done to improve.

The roles in the RACI chart are categorised for all processes as:

- Chief executive officer (CEO)
- Chief financial officer (CFO)
- Business executives
- Chief information officer (CIO)
- Business process owner
- Head operations
- Chief architect
- Head development
- Head IT administration (for large enterprises, the head of functions such as human resources, budgeting and internal control)
- The project management officer (PMO) or function
- Compliance, audit, risk and security (groups with control responsibilities but not operational IT responsibilities)

Certain specific processes have an additional specialised role specific to the process, e.g., service desk/incident manager for DS8.

It should be noted that while the material is collected from hundreds of experts, following rigorous research and review, the inputs, outputs, responsibilities, metrics and goals are illustrative but not prescriptive or exhaustive. They provide a basis of expert knowledge from which each enterprise should select what efficiently and effectively applies to it based on enterprise strategy, goals and policies.

Users of the COBIT Components

Management can use the COBIT material to evaluate IT processes using the business goals and IT goals detailed in appendix I to clarify the objectives of the IT processes and the process maturity models to assess actual performance.

Implementors and auditors can identify applicable control requirements from the control objectives and responsibilities from the activities and associated RACI charts.

All potential users can benefit from using the COBIT content as an overall approach to managing and governing IT, together with more detailed standards such as:

- ITIL for service delivery
- CMM for solution delivery
- ISO 17799 for information security
- PMBOK or PRINCE2 for project management

IT Governance Institute®

Leading the IT Governance Community

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*