COBIT® MAPPING

Mapping of ITIL v3 With COBIT® 4.1

LEADING THE IT GOVERNANCE COMMUNITY

IT Governance Institute®
The IT Governance Institute (ITGI™) (*www.itgi.org*) is a non-profit, independent research entity that provides guidance for the global business community on issues related to the governance of IT assets. ITGI was established by the non-profit membership association ISACA in 1998 to help ensure that IT delivers value and its risks are mitigated through alignment with enterprise objectives, IT resources are properly allocated, and IT performance is measured. ITGI developed *Control Objectives for Information and related Technology* (COBIT®) and Val IT™, and offers original research and case studies to help enterprise leaders and boards of directors fulfil their IT governance responsibilities and help IT professionals deliver value-adding services.

Disclaimer
ITGI has designed *COBIT® Mapping: Mapping of ITIL v3 With COBIT® 4.1* (the 'Work') primarily as an educational resource for control professionals. ITGI 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 proper information, procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific information, procedure or test, control professionals should apply their own professional judgement to the specific control circumstances presented by the particular systems or information technology environment.

IT Governance Institute
3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 USA
Phone: +1.847.660.5700
Fax: +1.847.253.1443
E-mail: *info@itgi.org*
Web site: *www.itgi.org*

ISBN 978-1-60420-035-5
COBIT® Mapping: Mapping of ITIL v3 With COBIT® 4.1
Printed in the United States of America

ACKNOWLEDGEMENTS

ITGI wishes to recognise:

Researchers
Jimmy Heschl, CISA, CISM, CGEIT, ITIL-SM, KPMG, Austria
Gary Hardy, IT Winners, South Africa

Expert Reviewers
Kelvin J. Arcelay, CISM, CISSP, HISP, PMP, Arcelay and Associates LLC, USA
Gary R. Austin, CISA, CISSP, PMP, CIA, CGFM, KPMG, USA
Johann Botha, Circle of Excellence, South Africa
Jeroen Bronkhorst, Hewlett-Packard Company, Netherlands
Jim Clinch, Clinch Consulting, UK
Monica Jain, CSQA, CSSBB, Covansys—A CSC Company, USA
John E. Jasinski, USA
Debra Mallette, CISA, CSSBB, Kaiser Permanente, USA
Mario Micallef, CPAA, FIA, National Australia Bank Group, Australia
John A. Mitchell, Ph.D., CISA, CFE, CITP, FBCS, FIIA, MBCS, MIIA, QiCA, LHS Business Control, England
Robert E. Stroud, CA Inc., USA
Anh Tran, CISA, BearingPoint Inc., USA
Allen Ureta, CISA, CISSP, GSEC, ITIL-SM, PMP, Ernst & Young LLP, USA

ITGI Board of Trustees
Lynn Lawton, CISA, FBCS CITP, FCA, FIIA, PIIA, KPMG LLP, UK, International President
Georges Ataya, CISA, CISM, CISSP, ICT Control sa-nv, Belgium, Vice President
Avinash Kadam, CISA, CISM, CBCP, CISSP, Miel e-Security Pvt. Ltd., India, Vice President
Howard Nicholson, CISA, City of Salisbury, Australia, Vice President
Jose Angel Pena Ibarra, Consultoria en Comunicaciones e Info., SA & CV, Mexico, Vice President
Robert E. Stroud, CA Inc., USA, Vice President
Kenneth L. Vander Wal, CISA, CPA, Ernst & Young LLP (retired), USA, Vice President
Frank Yam, CISA, FHKCS, FHKIoD, CIA, CCP, CFE, CFSA, FFA, Focus Strategic Group, Hong Kong, Vice President
Marios Damianides, CISA, CISM, CA, CPA, Ernst & Young LLP, USA, Past International President
Everett C. Johnson, CPA, Deloitte & Touche LLP (retired), USA, Past International President
Ronald Saull, CSP, Great-West Life Assurance and IGM Financial, Canada, Trustee
Tony Hayes, FCPA, Queensland Government, Australia, Trustee

IT Governance Committee
Tony Hayes, FCPA, Queensland Government, Australia, Chair
Max Blecher, Virtual Alliance, South Africa
Sushil Chatterji, Edutech, Singapore
Anil Jogani, CISA, FCA, Avon Consulting Ltd., UK
John W. Lainhart IV, CISA, CISM, CGEIT, IBM, USA
Lucio Molina Focazzio, CISA, Colombia
Ronald Saull, CSP, Great-West Life Assurance and IGM Financial, Canada
Michael Schirmbrand, Ph.D., CISA, CISM, CPA, KPMG, Austria
Robert E. Stroud, CA Inc., USA
John Thorp, CMC, ISP, The Thorp Network Inc., Canada
Wim Van Grembergen, Ph.D., University of Antwerp, University of Antwerp Management School, and IT Alignment and Governance (ITAG) Research Institute, Belgium

ACKNOWLEDGEMENTS (*CONT.*)

COBIT Steering Committee
Robert E. Stroud, CA Inc., USA, Chair
Gary S. Baker, CA, Deloitte & Touche, Canada
Rafael Eduardo Fabius, CISA, Republica AFAP SA, Uruguay
Urs Fischer, CISA, CIA, CPA (Swiss), Swiss Life, Switzerland
Erik Guldentops, CISA, CISM, University of Antwerp Management School, Belgium
Jimmy Heschl, CISM, CISA, CGEIT, KPMG, Austria
Debbie A. Lew, CISA, Ernst & Young LLP, USA
Maxwell J. Shanahan, CISA, FCPA, Max Shanahan & Associates, Australia
Dirk E. Steuperaert, CISA, IT In Balance BVBA, Belgium

ITGI Affiliates and Sponsors
ISACA chapters
American Institute of Certified Public Accountants
ASIS International
The Center for Internet Security
Commonwealth Association for Corporate Governance Inc.
FIDA Inform
Information Security Forum
Information Systems Security Association
Institut de la Gouvernance des Systemes d'Information
Institute of Management Accountants Inc.
ISACA
ITGI Japan
Socitm Performance Management Group
Solvay Business School
University of Antwerp Management School
Aldion Consulting Pte. Ltd.
Analytix Holdings Pty. Ltd.
Bwise B.V.
CA Inc.
Consult2Comply
Hewlett-Packard
IBM
ITpreneurs Nederlands B.V.
LogLogic Inc.
Phoenix Business and Systems Process Inc.
Project Rx Inc.
Symantec Corp.
TruArx Inc.
Wolcott Group LLC
World Pass IT Solutions

TABLE OF CONTENTS

1. PURPOSE OF THE DOCUMENT

The IT Governance Institute (*www.itgi.org*) exists to assist enterprise leaders in their responsibility to ensure that IT goals align with those of the business, IT delivers value, its performance is measured, its resources are allocated properly and its risks are mitigated. Through original research, case studies and electronic resources, ITGI helps ensure that boards and executive management have the tools and information they need for IT to deliver against expectations. One such tool is the COBIT framework. COBIT was initially created by the Information Systems Audit and Control Foundation® (ISACF®) in 1996. ITGI, which was founded by ISACA in 1998, released COBIT® 3rd Edition in 2000, COBIT® 4.0 in 2005 and COBIT® 4.1 in 2007. This series of COBIT mapping papers supports the effective use of COBIT in conjunction with a number of IT-related frameworks and standards.

COBIT provides a high-level, comprehensive IT governance and control framework based on the harmonisation of more than 50 IT good practice sources published by various international standards bodies, governments and other institutions.

ITGI has been conducting a research project that provides a detailed comparison between COBIT and a selection of these standards and good practices, to support ongoing COBIT developments and provide guidance to COBIT users implementing IT governance. The series of COBIT mapping papers supports the effective use of COBIT in conjunction with a number of IT-related frameworks and standards. The research addresses questions such as:

- What should be defined?
- What is an appropriate level of detail?
- What should be measured?
- What should be automated?
- What is good practice?
- Is there a certification available?

The results of the research project (the mapping papers) can be used to further enhance the definition of COBIT's control objectives and alignment with other good practices and standards. In addition, the results help entities that are planning to apply standards and guidance to harmonise those initiatives and use COBIT as the overall framework for sound IT governance.

Although many of these questions can be addressed using the openly available COBIT guidance, more specific information is sometimes required. The mapping project addresses the gaps by mapping the most important and commonly used standards[1] to the COBIT processes and control objectives. It consists of two components:

- A high-level overview of a variety of international standards and guidance, and a mapping of COBIT to IT Infrastructure Library (ITIL) and ISO 17799 (27002). These are posted on the ISACA web site at *www.isaca.org/cobitmapping*:
  - *COBIT® Mapping: Overview of International IT Guidance, 2nd Edition*
  - *Aligning COBIT®, ITIL and ISO 17799 for Business Benefit*
- A series of more detailed mapping documents focusing on individual standards or guidance is posted at *www.isaca.org/cobitmapping* and available from the ISACA Bookstore (*www.isaca.org/bookstore*):
  - *COBIT® Mapping: Mapping of CMMI® for Development V1.2 With COBIT® 4.0*
  - *COBIT® Mapping: Mapping of COSO Enterprise Risk Management With COBIT® 4.1*
  - *COBIT® Mapping: Mapping of ISO/IEC 17799:2000 With COBIT® 4.0, 2nd Edition*
  - *COBIT® Mapping: Mapping of ISO/IEC 17799:2005 With COBIT® 4.0*
  - *COBIT® Mapping: Mapping of ITIL With COBIT® 4.0*
  - *COBIT® Mapping: Mapping of NIST SP800-53 With COBIT® 4.1*
  - *COBIT® Mapping: Mapping of PMBOK© With COBIT® 4.0*
  - *COBIT® Mapping: Mapping of PRINCE2 With COBIT® 4.0*
  - *COBIT® Mapping: Mapping of SEI's CMM for Software With COBIT® 4.0*
  - *COBIT® Mapping: Mapping of TOGAF 8.1 With COBIT® 4.0*

Planned mappings include:

- *COBIT® Mapping: Mapping of FFIEC With COBIT® 4.1*
- *COBIT® Mapping: Mapping of PRINCE2 With COBIT® 4.1*
- *COBIT® Mapping: Mapping of ISO 20000 With COBIT® 4.1*
- *COBIT® Mapping: Mapping of TOGAF 9 With COBIT® 4.1*
- *COBIT® Mapping: Mapping of CMMI® for Development V1.2 With COBIT® 4.1*
- *COBIT® Mapping: Mapping of IT Baseline Protection Manual With COBIT® 4.1*
- *COBIT® Mapping: Mapping of PMBOK© With COBIT® 4.1*

[1] The term 'standard' is used in this document to encompass guidance publications.

- *COBIT® Mapping: Mapping of ISO/IEC 27002 With COBIT® 4.1*
- *COBIT® Mapping: Mapping of ISO/IEC 27005 With COBIT® 4.1*
- *COBIT® Mapping: Mapping of SEI's CMM for Software With COBIT® 4.1*
- *COBIT® Mapping: Overview of International IT Guidance, 3rd Edition*
- *Aligning COBIT®4.1, ITIL v3 and ISO 27002 for Business Benefit*

This document contains the results of a detailed mapping of ITIL v3 with COBIT 4.1 as well as a classification of the standards discussed in this publication, per the content of the overview document *COBIT Mapping: Overview of International IT Guidance, 2nd Edition*.

A brief overview of the standards mapped against each other in this document is as follows:
- **COBIT**—Released as an IT process and control framework linking IT to business requirements, COBIT initially was used mainly by the assurance community in conjunction with business and IT process owners. With the addition of management guidelines in 1998, COBIT was used more frequently as a management framework, providing management tools, such as metrics and maturity models, to complement the control framework. With the release of COBIT 4.0 in 2005, it became a more complete IT governance framework. Incremental updates to COBIT 4.0 were made in 2007; they can be seen as a fine-tuning of the framework, not fundamental changes. The current version is COBIT 4.1.
- **ITIL v3**—Released by the UK Office of Government Commerce (OGC), ITIL it is the most widely accepted approach to IT service management in the world. Version 3 consists of 27 detailed processes organised into five high-level processes described in five core books—*Service Strategy, Service Design, Service Transition, Service Operation* and *Continual Service Improvement*—that comprise one function: effective IT service management. In addition, ITIL v3 introduced the concept of the service life cycle and this is described in the book *Official Introduction to the IT Service Lifecycle*.

This mapping does not contain all of the details of ITIL v3. Some language is included directly from ITIL, but it is recommended to obtain a copy of the original document. The document is available from OGC's web site, *www.ogc.gov.uk*.

2. METHODOLOGY FOR THE MAPPING

The mapping is performed in two layers. A high-level mapping compares the components of ITIL v3 with the components of COBIT and shows the coverage of IT governance focus areas. The detailed mapping was done as shown in **figure 1**.

Figure 1—Detailed Mapping Process

Step	Description
1	Core control information was identified from each of the 27 ITIL v3 processes, which were mapped to one or more COBIT control objectives. Those pieces of information are called 'information requirements'.
2	The information requirements were mapped to COBIT control objectives as follows: a. A 1:1 mapping was done for information requirements that fit to a single control objective. b. A 1:n mapping was done for information requirements that fit to more than one control objective. c. If the information requirement covers a complete COBIT process, it was mapped to the respective COBIT process (control objective n.n, e.g., DS5.1) d. If a, b and c failed, then COBIT does not cover the requirement of this specific information, in which case the most appropriate process was selected and the information requirement was mapped to (non-existent) control objective 99 of the process.
3	The requirements described by the information requirements were detailed from ITIL v3, and the results sorted as defined by the COBIT framework.

The information resulting from step 3 will help implementers and auditors using the COBIT framework to determine if they properly consider the requirements of ITIL v3.

3. CobiT Overview

DOCUMENT TAXONOMY

CobiT represents a collection of documents that can be classified as generally accepted good practices for IT governance, control and assurance.

ISSUER

The first edition of CobiT was issued by ISACF in 1996. In 1998, the second edition was published with additional control objectives and the *Implementation Tool Set*. The third edition was issued by ITGI in 2000 and included the management guidelines and several new control objectives. In 2005, ITGI finalised a complete rework of the CobiT content and published CobiT 4.0, which demonstrated a clear focus on IT governance. The current version, CobiT 4.1, includes incremental updates.

GOAL OF THE GUIDANCE

The CobiT mission is:

> *…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*.[2]

BUSINESS DRIVERS FOR IMPLEMENTING THE GUIDANCE, INCLUDING TYPICAL SITUATIONS

CobiT usually is implemented subject to one or more of the following business cases:
- There is a need for IT governance.
- Services delivered by IT are to be aligned with business goals.
- IT processes are to be standardised/automated.
- A framework for overall IT processes is needed.
- IT processes are to be unified.
- A framework is needed for a quality management system for IT.
- A structured audit approach is to be defined.
- Mergers and acquisitions with an IT impact are occurring.
- IT cost-control initiatives are desired.
- Part or all of the IT function is to be outsourced.
- Compliance with external requirements (e.g., regulators, organisations or third parties) is of concern.
- Important changes in an organisation, its business goals and processes affect IT.

RELATED RISKS OF NOT IMPLEMENTING THE GUIDANCE

Risks of not implementing CobiT include:
- Misaligned IT services and divergence
- Weak support of business goals due to misalignment
- Wasted opportunities due to misalignment
- Persistence of the perception of IT as a black box
- Shortfall between management's measurements and expectations
- Know-how tied to key individuals, not to the organisation
- Excessive IT cost and overhead
- Erroneous investment decisions and projections
- Dissatisfaction of business users with IT services supplied
- Regulatory breaches with potential significant financial penalties on organisations, restrictions on operating licences, and fiduciary liability on directors and officers if deemed not to have exercised due care and responsibility
- Unfulfilled information criteria
- Adverse effects on the organisation's internal control system due to a weak enterprise architecture for IT

[2] IT Governance Institute, CobiT® 4.1, USA

TARGET AUDIENCE

All types of organisations, public and private companies, and external assurance and advisory professionals form the relevant target group. Within organisations, COBIT intends to support executive management and boards; business and IT management; and governance, assurance, control and security professionals. The level of detail primarily depends on the role of the function. If the function is responsible to fulfil the requirements, thorough knowledge should be ensured, but if the function is accountable or involved otherwise (consulted or informed), an overview should be applicable. The level is indicated in **figure 2**.

Figure 2—Chart of COBIT Audiences

	Functions: Thorough knowledge of the document (T), and overview of the document's intention and content (O)										
	Chief Executive Officer (CEO)	Chief Financial Officer (CFO)	Business Executive	Chief Information Officer (CIO)	Business Process Owner	Head of Operations	Chief Architect	Head of Development	Head of IT Administration	Project Management Office	Compliance, Audit, Risk and Security
COBIT	O	O	O	T	O	O	O	O	O	O	T
Plan and Organise	O	O	O	T	O	O	T		T	T	
Acquire and Implement				O	O	O	T	T	O	T	O
Deliver and Support				O	O	T	O	O	T	O	O
Monitor and Evaluate	O	O	O	T	O	O	O	O	T	O	O

TIMELINESS

The core content of COBIT was updated in 2005, resulting in COBIT 4.0, and was further refined in 2007, resulting in COBIT 4.1. The research conducted for these updates addressed components of the control objectives and management guidelines. Specific areas that were addressed include:

- COBIT—IT governance bottom-up and top-down alignment
- COBIT and other detailed standards—Detailed mapping between COBIT and ITIL v2,[3] CMM,[4] COSO,[5] PMBOK,[6] ISF's *Standard of Good Practice for Information Security*,[7] ISO/IEC 27000 series,[8] and other global and regional frameworks and standards, to enable harmonisation with those standards in language, definitions and concepts
- Review of the quality of the critical success factors (CSFs)—CSFs were replaced by process inputs (success factors needed from others) and activity goals (goals that the process owner must address).
- Review of CSF content—Splitting the CSFs into 'what you need from others' and 'what you need to do yourself'
- Linking of business goals, IT goals and IT processes—Detailed research was conducted in eight different industries, resulting in more detailed insight into how COBIT processes support the achievement of specific IT goals and, by extension, business goals.
- Review of maturity models' content—Ensured consistency and quality of maturity levels between and within processes, including better definitions of maturity model attributes

Also, the range of COBIT-related products was expanded in 2007 to include *IT Assurance Guide: Using COBIT®, IT Governance Implementation Guide: Using COBIT® and Val IT™, 2nd Edition,* and *COBIT® Control Practices, 2nd Edition*.

[3] British Office of Government Commerce (OCG®), IT Infrastructure Library® (ITIL), UK, 1999-2004
[4] Software Engineering Institute (SEI) of Carnegie Mellon University, Capability Maturity Model for Software (CMM), USA, 1993, and Capability Maturity Model Integration (CMMI®), 2000
[5] Committee of Sponsoring Organisations of the Treadway Commission (COSO), *Internal Control—Integrated Framework, USA, 1994,* and *Enterprise Risk Management—Integrated Framework*, 2004
[6] Project Management Institute, *A Guide to the Project Management Body of Knowledge (PMBOK), 3rd Edition*, 2004
[7] Information Security Forum (ISF), *Standard of Good Practice for Information Security*, UK, 2003
[8] International Organisation for Standardisation (ISO)/International Electrotechnical Commission (IEC), 27000 (Series working title: *Information Technology—Security Techniques—Information Security Management Systems—Overview and Vocabulary)*, Switzerland. The first document, 27001, was published in 2005. 27002 and 27006 were issued in 2007. Others are still in development.

CERTIFICATION OPPORTUNITIES

The *IT Assurance Guide* is aligned with COBIT 4.1 and can be used for auditing and self-assessment against the control objectives, but there is no certification for organisations. However, the COBIT framework is used frequently by Certified Public Accountants (CPAs) and Chartered Accountants (CAs) when performing a Statement on Auditing Standards (SAS) No. 70 service organisation review, earning SysTrust certification or pursuing Sarbanes-Oxley compliance.

Individuals can complete the COBIT Foundation Course™ and obtain a certificate of completion. Non-COBIT-specific certification is available through ISACA, ITGI's affiliated association, in the form of the Certified Information Systems Auditor™ (CISA®), Certified Information Security Manager® (CISM®) and Certified in the Governance of Enterprise IT™ (CGEIT™) certifications.

CIRCULATION

COBIT is used worldwide. In addition to the English version, COBIT has been translated into French, German, Hebrew, Hungarian, Italian, Japanese, Korean, Portuguese and Spanish. Further translations (Czech, Turkish) and updates of translations to COBIT 4.1 are in development.

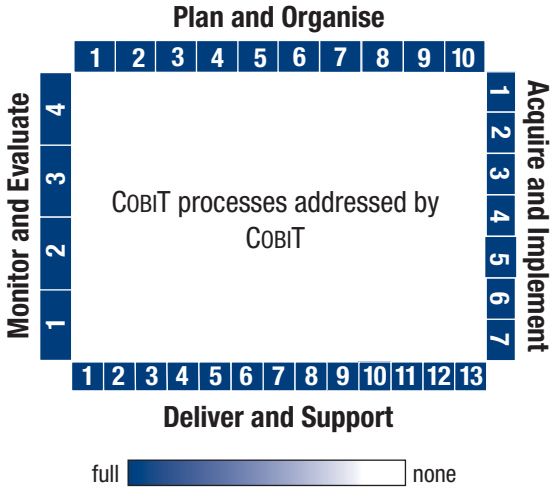
COMPLETENESS

COBIT addresses a broad spectrum of duties in IT management. It includes the most significant parts of IT management, including those covered by other standards. Although no technical details are included, the necessary tasks for complying with the control objectives are self-explanatory. Therefore, it is classified at a relatively high level, aiming to be generically complete but not specific.

AVAILABILITY

COBIT 4.1 is readily accessible for complimentary electronic download from the ITGI or ISACA web sites, *www.itgi.org/cobit* or *www.isaca.org/cobit*. COBIT Online® can be purchased at *www.isaca.org/cobitonline*. COBIT Online allows users to customise a version of COBIT just right for their own enterprise, then store and manipulate that version as desired. It offers online, real-time surveys and benchmarking. *IT Assurance Guide: Using COBIT* is posted on the ISACA site for complimentary download for ISACA members. Alternatively, the print versions of COBIT 4.1 and most related publications be purchased from the ISACA Bookstore, *www.isaca.org/bookstore*.

COBIT PROCESSES ADDRESSED



Note: The chart is not a comparison; this is COBIT itself.

INFORMATION CRITERIA ADDRESSED

Information Criteria
+ Effectiveness
+ Efficiency
+ Confidentiality
+ Integrity
+ Availability
+ Compliance
+ Reliability

(+) Frequently addressed
(o) Moderately addressed
(-) Not or rarely addressed

Note: The chart is not a comparison, this is COBIT itself.

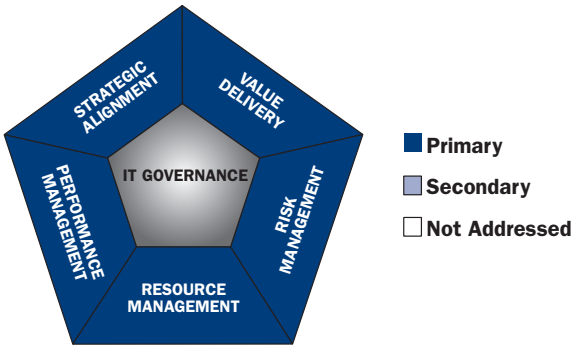
IT RESOURCES CONCERNED

IT Resources
+ Applications
+ Information
+ Infrastructure
+ People

(+) Frequently addressed
(o) Moderately addressed
(-) Not or rarely addressed

Note: This chart is not a comparison, this is COBIT itself.

IT GOVERNANCE FOCUS AREAS ADDRESSED



DESCRIPTION OF THE GUIDANCE AND ITS CONTENT

Enterprise governance (the system by which organisations are governed and controlled) and IT governance (the system by which the organisation's IT is governed and controlled) are, from a COBIT point of view, highly related. Enterprise governance is inadequate without IT governance and *vice versa*. IT can extend and influence the performance of the organisation, but IT has to be subject to adequate governance. On the other hand, business processes require information from the IT processes, and this interrelationship has to be governed as well.

In this subject matter, the plan-do-check-act (PDCA) cycle becomes evident. The concept of the PDCA cycle usually is used in structured problem-solving and continuous-improvement processes. The PDCA cycle is also known as the Deming cycle or the Deming wheel of a continuous improvement process. Both the information needed (enterprise governance) and the information delivered (IT governance) have to be planned with measurable and constructive indicators (plan). The information and, possibly, information systems have to be implemented, delivered and used (do). The outcome of the information delivered and used is measured against the indicators defined in the planning phase (check). Deviation is investigated, and corrective action is taken (act).

Considering these interdependencies, it is apparent that the IT processes are not an end in themselves; instead, they are a means to an end that is highly integrated with the management of business processes.

IT GOVERNANCE USING CobiT

ITGI has defined IT governance as follows:

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.[9]

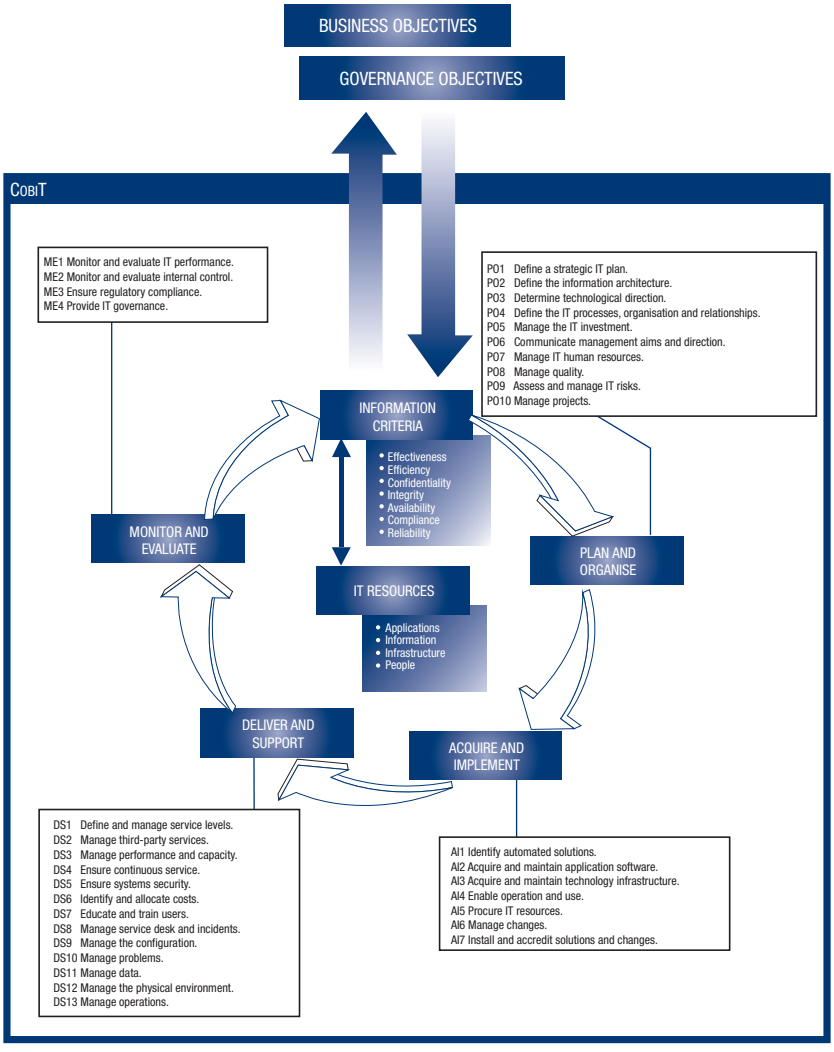
CobiT supports IT governance by providing a framework to ensure that:
- IT is aligned with the business
- IT enables the business and maximises benefits
- IT resources are used responsibly
- IT risks are managed appropriately

Performance measurement is essential for IT governance, is supported by CobiT, and includes setting and monitoring measurable objectives of what IT processes need to deliver (process outcome) and how they deliver it (process capability and performance).

THE CobiT IT PROCESSES

The CobiT processes are grouped into four domains, as indicated in **figure 3**.

Figure 3—CobiT IT Processes Defined Within the Four Domains



[9] ITGI, *Board Briefing on IT Governance, 2nd Edition*, 2003, p. 10

Any service delivered by IT and all services provided to the core processes have to be integrated into the IT service life cycle, as indicated in **figure 3**. Plans and organisational structures already developed can be adopted, depending on the significance of each service, rather than developing a new plan for the IT service. Services are implemented subsequently, and all necessary precautions for ongoing service, delivery and monitoring are considered.

From the IT governance point of view, single services are merely in the background. The focus must be on the PDCA cycle discussed previously, for the sum of services delivered by and with IT.

Each process is described by using the following information:
- A process description
- Control objectives
- Information criteria affected by the process
- IT resources used by the process
- IT governance focus areas
- Inputs and outputs
- A Responsible, Accountable, Consulted and Informed (RACI) chart
- Goals and metrics

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.
- **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 those 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.

IT RESOURCES

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

MATURITY MODELS

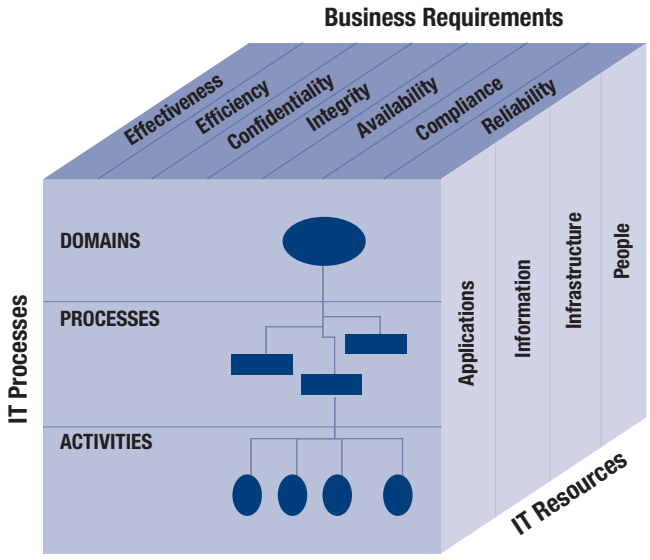
Maturity modelling for management and control over IT processes is based on a method of self-evaluation by the organisation. A maturity model has been defined for each of the 34 COBIT IT processes, providing an incremental measurement scale from 0, non-existent, through 5, optimised. Using the maturity models developed for each IT process, 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 maturity attributes list the characteristics of how IT processes are managed and describe 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. The maturity attributes are:
- Awareness and communication
- Policies, plans and procedures
- Tools and automation
- Skills and expertise
- Responsibility and accountability
- Goal setting and measurement

CobiT CUBE

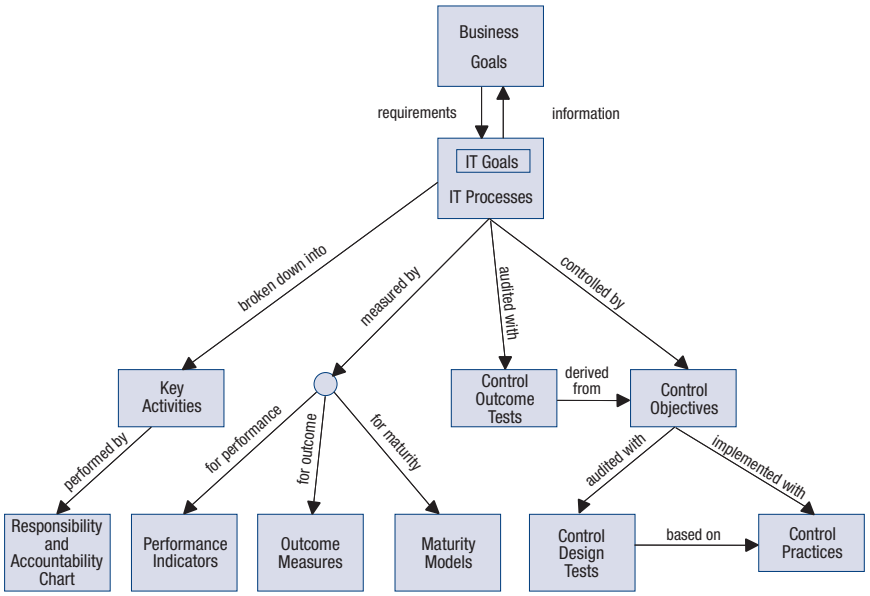
The previously mentioned components (IT processes, business requirements of information and resources) are three-dimensional, thus illustrating the IT function. These dimensions, shown in **figure 4**, represent the CobiT cube.

Figure 4—CobiT Cube



The COBIT components interrelate, as shown in **figure 5**.

Figure 5—Interrelationships of COBIT Components



Source: COBIT 4.1, Figure 4—Interrelationships of COBIT Components, p. 8

The IT processes and control objectives, activity goals, performance drivers, outcome measures and maturity models are documented in COBIT 4.1.

For more information, refer to the appendix, COBIT and Related Products.

FURTHER REFERENCES

Internet	
ISACA	*www.isaca.org/cobit*
ITGI	*www.itgi.org/cobit*

4. ITIL v3 Overview

DOCUMENT TAXONOMY

ITIL v3 is a series of six books and is referred to as the only consistent and comprehensive best practice for IT service management to deliver high-quality IT services. Although produced and published by a single governmental body (it is owned by the British government), ITIL is not a standard. The books are titled:
- *Service Strategy*
- *Service Design*
- *Service Transition*
- *Service Operation*
- *Continual Service Improvement*
- *Official Introduction to the ITIL Service Lifecycle*

ISSUER

This mapping publication focuses on the first five books. The ITIL collection was first published by the Central Computer and Telecommunications Agency (CCTA), now the British Office of Government Commerce (OGG), which holds the ITIL copyright and trademark. The OGC was commissioned to develop a methodology for efficient and effective use of IT resources within the British government.

GOAL OF THE GUIDANCE

The goal is the development of a vendor-independent approach for service management. The ethos behind the development was the recognition of increased dependence on IT service, which has to be managed by high-quality IT processes.

BUSINESS DRIVERS FOR IMPLEMENTING THE GUIDANCE, INCLUDING TYPICAL SITUATIONS

ITIL is usually implemented subject to one or more of the following drivers:
- Service processes within an enterprise's IT function or within a service provider's organisation need to be defined.
- The quality of services needs to be defined and improved.
- There is a need to focus on the customer of the IT services.
- There is a need to implement specific IT service management tasks such as creation of a service desk function and service level, incident, problem, and availability management.
- It is necessary to mitigate the risk of implementing a service management system that does not work (right away).
- The predictability of services and service delivery (warranty) needs improvement.

RELATED RISKS OF NOT IMPLEMENTING THE GUIDANCE

Risks of not implementing ITIL include:
- Inefficient services provided to users and customers
- Unclear services and processes
- Inefficient and ineffective communication of service delivery objectives
- Lack of common language for IT service delivery and service support
- Inappropriate priority given to different services provided
- Dissatisfaction of users and customers with services provided
- Ineffective planning and maintenance of services and required resources
- Misalignment of IT services and business requirements

TARGET AUDIENCE

The level of detail primarily depends on the role of the function. If the function is responsible to fulfil the requirements, thorough knowledge should be ensured, but if the function is accountable or involved otherwise (consulted or informed), an overview should be applicable. The level is indicated in **figure 6**.

Figure 6—Chart of ITIL v3 Audiences

	Functions: Thorough knowledge of the document (T), and overview of the document's intention and content (O)										
	Chief Executive Officer (CEO)	Chief Financial Officer (CFO)	Business Executive	Chief Information Officer (CIO)	Business Process Owner	Head of Operations	Chief Architect	Head of Development	Head of IT Administration	Project Management Office	Compliance, Audit, Risk and Security
ITIL v3	O			O	O	O	O	O	O	O	O
Service Strategy	O	O	O	T	O	O			O		
Service Design			O	O	O	O	T	T	O	O	O
Service Transition				O	O	O	T	T	O	O	O
Service Operation				O		T	O	O	O		O
Continual Service Improvement				T	O	O	O	O	T		O

TIMELINESS

ITIL v1 (focused on managing technology) was created in the 1980s and ITIL v2 (focused on implementing service management processes) in the 1990s. The ITIL v3 publications were released in mid-2007 following a very extensive development effort over several years based on feedback from users of the previous ITIL versions.

CERTIFICATION OPPORTUNITIES

Certification of personnel is available under ITIL, but the programme is going through an extensive revision process to reflect the new guidance in v3. There are also conversion courses and exams that previously certified personnel must complete to retain their certification. There are three levels of certification for IT service management staff at different functional levels.

Organisations can be certified under ISO/IEC 20000, which presents a specification for IT service management for which selected ITIL processes can be used as guidance documents. Note that ISO 27001/2 complies with the security requirements of ISO/IEC 20000.

CIRCULATION

ITIL is used internationally and is available in several languages.

COMPLETENESS

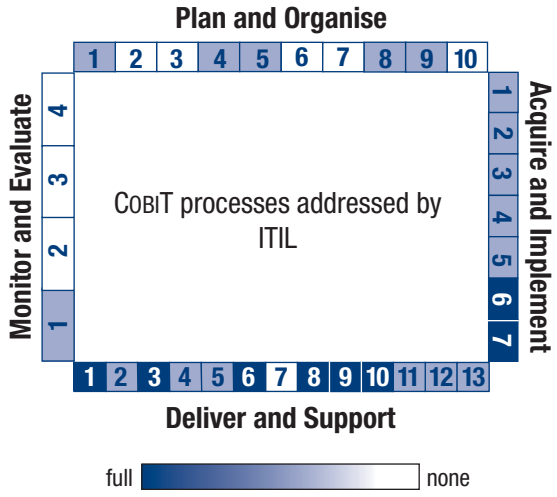
The ITIL books examine and describe IT service management processes in extensive detail (more than 1,500 pages) and v3 introduces two new books, *Service Strategy* and *Continuous Service Improvement*, covering the life cycle of IT management from the perspective of IT services. It does not attempt to cover the entire breadth of IT management and IT governance.

Most of the processes of the COBIT Deliver and Support (DS) domain are covered in a comprehensive manner. Processes of the Plan and Organise (PO), Acquire and Implement (AI) and Monitor and Evaluate (ME) domains are partially covered, with the focus on services.

AVAILABILITY

ITIL v3 is available for purchase in paperback and also for online access via OGC's publishers, The Stationery Office (TSO), at *www.best-management-practice.com*.

CobiT PROCESSES ADDRESSED



INFORMATION CRITERIA ADDRESSED

Information Criteria
+ Effectiveness
+ Efficiency
o Confidentiality
o Integrity
o Availability
- Compliance
- Reliability

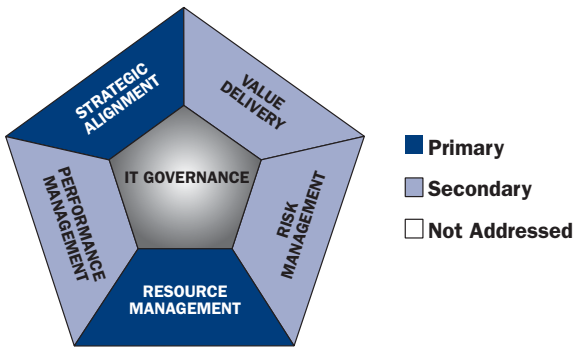
(+) Frequently addressed
(o) Moderately addressed
(-) Not or rarely addressed

IT RESOURCES CONCERNED

IT Resources
+ Applications
o Information
+ Infrastructure
+ People

(+) Frequently addressed
(o) Moderately addressed
(-) Not or rarely addressed

IT GOVERNANCE FOCUS AREAS ADDRESSED



DESCRIPTION OF GUIDANCE AND ITS CONTENT

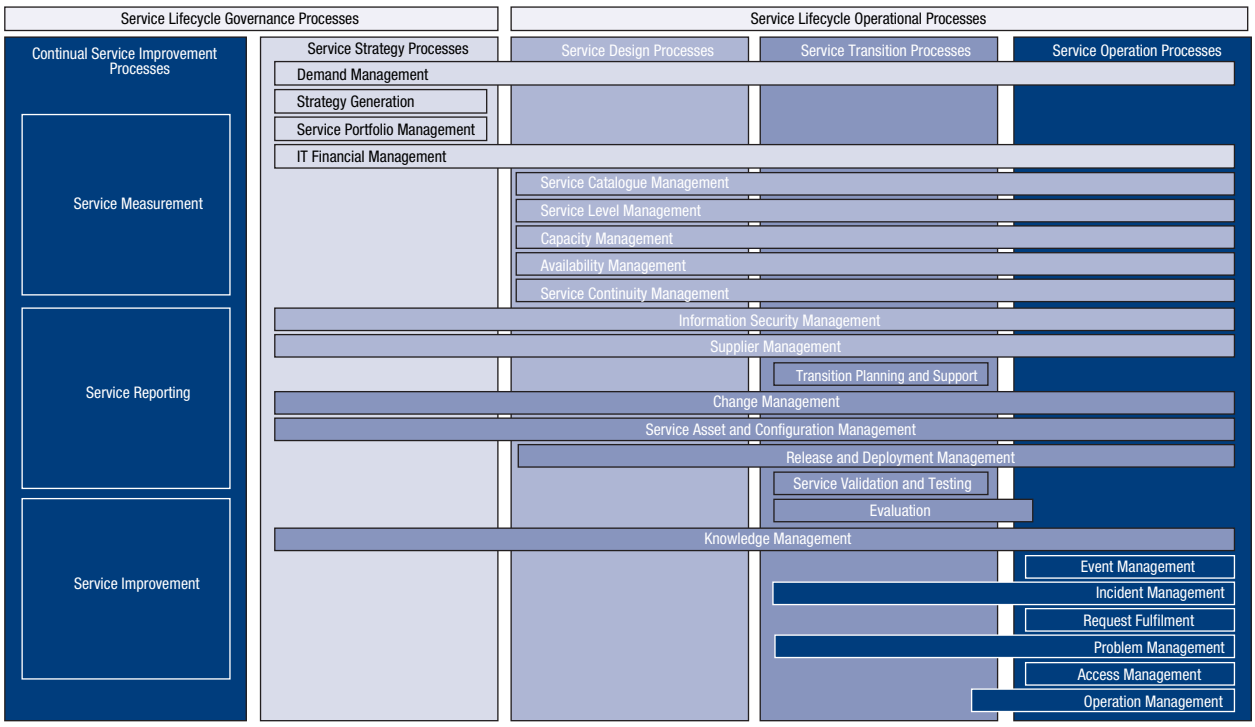
The five core books of ITIL v3 are:

- ***Service Strategy*** **(SS)**—Covers the strategic planning of service management capabilities and the alignment of service and business strategies. Furthermore, it provides guidance on value creation, market and offerings strategies, structure of services, types of service providers, organisational development, sourcing, and financial management. It outlines four key processes: demand management, strategy generation, service portfolio management and IT financial management.
- ***Service Design*** **(SD)**—Outlines the design and development of services and service management processes. Processes covered by this volume are service catalogue management, service-level management, capacity and availability management, IT service continuity management, information security management, and supplier management. It identifies availability management, capacity management, continuity management and security management as key elements used in the design of the services to be provided.
- ***Service Transition*** **(ST)**—Illustrates how the requirements of previous stages (strategy and design) are realised and how capabilities for the ongoing delivery of a service can be maintained. The processes covered are transition planning and support, change management, service asset and configuration management, release and deployment management, service validation and testing, and evaluation and knowledge management.
- ***Service Operation*** **(SO)**—Covers the effective and efficient delivery and support of services, and provides a benchmarked approach for event management, incident management, request fulfillment, problem management and access management. It also provides references to operational activities in other processes.
- ***Continual Service Improvement*** **(CSI)**—Covers ongoing improvement of the service and the measurement of process performance required for the service. There are three key areas: service measurement, service reporting and service improvement. The principles of CSI are covered in a seven-step improvement process.

The processes described in ITIL v3 follow a similar, but not always consistent, structure:

- Purpose, goals and objective
- Scope
- Value to the business
- Policies, principles and basic concepts
- Process activities, methods and techniques
- Triggers, inputs, outputs and (interprocess) interfaces
- Key performance indicators (KPIs) or metrics
- Challenges, critical success factors (CSFs) and risks

Figure 7—Service Life Cycle Governance and Operational Elements



Source: ITIL v3, *Official Introduction to the ITIL Service Lifecycle*, figure 10.2. Reprinted with permission.

FURTHER REFERENCES

Internet	
OGC	*www.ogc.gov.uk*
Best Management Practice	*www.best-management-practice.com*
ITIL	*www.itil.co.uk*

5. HIGH-LEVEL MAPPING

OVERVIEW

Figure 8 is an overview of ITIL v3 and COBIT and highlights the differences in guidance.

Figure 8—ITIL v3 Processes Mapped to High-level COBIT Processes

COBIT 4.1 Processes and Domains	1	2	3	4	5	6	7	8	9	10	11	12	13
Plan and Organise	o	-	-	o	o	-	-	o	o	-	\	\	\
Acquire and Implement	o	o	o	o	o	+	+	\	\	\	\	\	\
Deliver and Support	+	o	+	o	o	+	-	+	+	+	o	o	o
Monitor and Evaluate	o	-	-	-	\	\	\	\	\	\	\	\	\
Process Controls	-	o	-	o	+	+	\	\	\	\	\	\	\
Application Controls	o	o	o	o	o	+	\	\	\	\	\	\	\

(+) Significant match
(o) Minor match
(-) Unrelated or minor focus
(\) No COBIT IT process exists.

STRUCTURAL COMPARISON

Figure 9 shows a structural analysis and comparison of components used in ITIL v3 and COBIT for the process definitions. Please note that for this mapping only the process activities, methods and techniques were mapped to the COBIT control objectives or processes, since other components do not have a link to those elements.

Figure 9—Process Definition Comparisons

	ITIL Process Subchapter	COBIT 4.1 Component
1	Purpose/goal/objective	Process description
2	Scope	Process description
3	Value to the business	Process description Management guideline Value driver
4	Policies, principles and basic concept	Process description Management guideline Control objective
5	Process activity, method and technique	Management guideline Control objective Control practice Maturity model
6	Trigger, input, output and interface	Management guideline
7	KPIs	Management guideline
8	Information management	Process description Management guideline Control objective
9	Challenge, CSFs and risk	Management guideline Risk driver

COVERAGE OF IT GOVERNANCE FOCUS AREAS

Figure 10 lists the coverage of IT governance focus areas.

Figure 10—Coverage of IT Governance Focus Areas

Focus Area	Coverage by COBIT	Coverage by ITIL v3
Strategic alignment	Requirements of this focus area can be covered by implementing the COBIT processes. Processes with a primary impact on this focus area are: • PO1 Define a strategic IT plan • PO2 Define the information architecture • PO6 Communicate management aims and direction • PO7 Manage IT human resources • PO8 Manage quality • PO9 Assess and manage IT risks • PO10 Manage projects • AI1 Identify automated solutions • AI2 Acquire and maintain application software • DS1 Define and manage service levels • ME3 Ensure compliance with external requirements • ME4 Provide IT governance These processes ensure that the IT-enabled initiatives are planned and organised in a structured manner and initiated appropriately. In addition, the delivery of IT services meets business and regulatory requirements and enables management and the business to oversee the service development and service delivery.	ITIL v3 provides useful guidance on strategic alignment of service strategies, particularly how to understand the business requirements, the potential demand on capacity, and how to organise services in a portfolio to ensure balance and prioritisation of resources. It also helps to understand the options for choosing service providers and how to decide sourcing strategies. Furthermore, it describes the four key processes of demand management, strategy generation, service portfolio management and IT financial management. Those topics are addressed primarily in the book *Service Strategy*.
Value delivery	Requirements of this focus area can be covered by implementing the COBIT processes. Processes with a primary impact on this focus area are: • PO5 Manage the IT investment • AI1 Identify automated solutions • AI2 Acquire and maintain application software • AI4 Enable operation and use • AI6 Manage changes • AI7 Install and accredit solutions and changes • DS1 Define and manage service levels • DS2 Manage third-party services • DS4 Ensure continuous service • DS7 Educate and train users • DS8 Manage service desk and incidents • DS9 Manage the configuration • DS10 Manage problems • DS11 Manage data • ME2 Monitor and evaluate internal control • ME4 Provide IT governance These processes ensure that IT-enabled business initiatives deliver value to the business by proper planning of the implementation, delivery of knowledge to ensure beneficial usage of services and providing a proper support for the services required in line with the business requirements.	Value delivery is addressed in two ways. In the strategy, design and transition of the life cycle, the value of services to the business is covered. The value of continuous improvement and process improvement is addressed in the continuous service improvement phase, with a focus on improvement of IT processes. Value to the business is discussed explicitly in every process described in the library.

Figure 10—Coverage of IT Governance Focus Areas (*cont.*)		
Focus Area	**Coverage by COBIT**	**Coverage by ITIL v3**
Resource management	Requirements of this focus area can be covered by implementing the COBIT processes. Processes with a primary impact on this focus area are: • PO2 Define the information architecture • PO3 Determine technological direction • PO4 Define the IT processes, organisation and relationships • PO7 Manage IT human resources • AI3 Acquire and maintain technology infrastructure • AI5 Procure IT resources • DS1 Define and manage service levels • DS3 Manage performance and capacity • DS6 Identify and allocate costs • DS9 Manage the configuration • DS13 Manage operations • ME4 Provide IT governance These processes are responsible for ensuring that IT is able to provide the resources required to deliver the services by focusing on planning and managing resources such as applications, information, infrastructure, and people.	Resource management is addressed in various places in all five books throughout the service management life cycle, from strategy to operation. The focus is mostly on infrastructure resource, helping to ensure that resources are used cost-effectively when delivering services, and specifically with the maintenance of accurate and up-to-date asset information in a configuration repository.
Risk management	Requirements of this focus area can be covered by implementing the COBIT processes. Processes with a primary impact on this focus area are: • PO4 Define the IT processes, organisation and relationships • PO6 Communicate management aims and direction • PO9 Assess and manage IT risks • DS2 Manage third-party services • DS4 Ensure continuous service • DS5 Ensure systems security • DS11 Manage data • DS12 Manage the physical environment • ME2 Monitor and evaluate internal control • ME3 Ensure compliance with external requirements • ME4 Provide IT governance These processes ensure that risks are identified and managed in a way that enables business and top management to understand the relevance of IT-related risks, implications on business risks and the adequacy of measures to control risks.	Risk management is addressed in various places in all five books throughout the service management life cycle, from strategy to operation. The focus is mostly on service availability, effectiveness and efficiency-related risks.
Performance measurement	Requirements of this focus area can be covered by implementing the COBIT processes. Processes with a primary impact on this focus area are: • PO8 Manage quality • DS1 Define and manage service levels • ME1 Monitor and evaluate IT performance • ME4 Provide IT governance These processes ensure that the previous focus areas (strategic alignment, value delivery, resource management and risk management) will achieve their desired outcomes. This creates the opportunity to take timely corrective measures, if needed.	*Continual Service Improvement* covers ongoing improvement of the service and the measurement of process performance required for the service. There are three key processes: service measurement, service reporting and service improvement. The principles of CSI are covered in a seven-step improvement process.

COMBINATION OF COBIT AND ITIL V3

COBIT is a proven set of good practices and processes that businesses can use to ensure that IT is working as effectively as possible to minimise IT-related risks and maximise the benefits of technology investment. It is a proactive, uniquely comprehensive management approach to ensuring that IT is meeting the needs of a business. The framework helps to document an IT department's ideal practices in a comprehensive, integrated manner and provides tools to measure, monitor and benchmark performance based on goals, metrics and maturity models. It helps IT show its value to the organisation, and it easily integrates with, and builds on, other business and IT frameworks, while improving their impact.

ITIL provides a comprehensive and very detailed set of good practices for the specific scope of IT service management and its related processes, promoting a quality approach for achieving business effectiveness and efficiency in the provision of IT services. The ITIL core books contain more than 1,500 pages of guidance and examples of how to define, design and deliver 27 key processes related to service management. In developing ITIL v3, the OGC performed an extensive survey to identify user requirements. One consequence resulting from the survey was a desire to strengthen the linkage to COBIT and improve the coverage of IT governance and business alignment. The new *Service Strategy* and *Continual Service Improvement* books have made considerable progress in this area. A comparison between ITIL's scope and COBIT's shows that many COBIT processes are covered, but the focus is always on service management. For example, with regard to the Plan and Organise domain of COBIT, ITIL's orientation is toward the service aspect of IT rather than new developments, with portfolio management specifically oriented toward services rather than programmes of projects. Similarly, in the AI domain, the focus is on AI4, AI5, AI6 and AI7 since these are related to the transition of services into operations, but the scope is on the services and the related infrastructure rather than on the applications.

When used together, COBIT and ITIL provide a top-to-bottom approach to IT governance and, thus, service management. COBIT guides management's priorities and objectives within a holistic and complete approach to a full range of IT activities. This can focus all stakeholders (business and IT management, auditors, and IT professionals) on an integrated and common approach. ITIL supports this with best practices for service management. When used together, the power of both approaches is amplified, with a greater likelihood of management support and direction, and a more cost-effective use of implementation resources.

ISO/IEC 20000 can also be considered when implementing ITIL, especially for service providers, and IS0 27001 provides guidance on security. OGC publishes several best practices and guidance documents that complement ITIL, such as PRINCE2 and the *Management of Risk Framework*.

RECOMMENDATIONS

Prioritising

To avoid costly and unfocused implementations of standards and good practices, organisations need to prioritise where and how to use standards and good practices. The organisation needs an effective action plan that suits its particular circumstances and needs. First, it is important for the board to take ownership of IT governance and set the direction management should follow. This is best accomplished by making sure that the board operates with IT governance in mind. The board should:

- Make sure IT is on the agenda
- Challenge management's activities with regard to IT to make sure that IT issues are uncovered
- Guide management by helping align IT initiatives with real business needs and ensure that management appreciates the potential impact on the business of IT-related risks
- Insist that IT performance be measured and reported to the board
- Establish an IT steering group or IT governing council with responsibility for communicating IT issues between the board and management
- Insist that there be a management framework for IT governance based on a common approach (e.g., COBIT) and a best practice framework for IT service management based on a global *de facto* standard (e.g., ITIL)

Planning

With this mandate and direction in place, management then can initiate and put into action an implementation approach. To help management decide where to begin and to ensure that the implementation process delivers positive results where they are needed most, the following steps are suggested:

1. Set up an organisational framework (ideally as part of an overall IT governance initiative) with clear responsibilities and objectives. Secure participation from all the interested parties that will progress implementation and own it as an initiative.
2. Align IT strategy with business goals. Determine the current business objectives in which IT has a significant contribution. Obtain a good understanding of the business environment, risk appetite and business strategy as they relate to IT. COBIT's management guidelines (specifically the goals and metrics) and COBIT's framework information criteria help define IT objectives. Used in conjunction with ITIL, services and service level agreements (SLAs) can be defined in end-user terms.

3. Understand and define the risks. Given the business objectives, what are the risks relating to IT's ability to deliver against these objectives? Consider:
   – Previous history and patterns of performance
   – Current IT organisational factors
   – The complexity and size/scope of the existing or planned IT environment
   – The inherent vulnerability of the current and planned IT environment
   – The nature of the IT initiatives being considered, e.g., new systems projects, outsourcing considerations, architectural changes, etc.
   COBIT's process for risk management (PO9) and the application of the COBIT control framework and information criteria help ensure that risks are identified and owned. Instituting ITIL clarifies operational risks, and ISO 27002 clarifies security risks.
4. Define target risk areas and identify the process areas in IT that are critical to managing the risk areas. The COBIT process framework can be used as the basis, underpinned by ITIL's definition of key service delivery processes. OGC's publication, *Management of Risk: Guidance to Practioners*, can also be of assistance in assessing and managing risks at any of the four main levels, i.e., strategic, programme, project or operational.
5. Analyse current capability and identify gaps. Perform a maturity capability assessment to find out where improvements are needed most. The COBIT management guidelines provide a basis, supported in more detail by ITIL best practices.
6. Develop improvement strategies, and decide which are the highest priority projects that will help improve the management and governance of these significant areas. This decision should be based on the potential benefit and ease of implementation, and should include a focus on important IT processes and core competencies. Outline specific improvement projects as part of a continuous improvement initiative.
7. Consider supporting the COBIT control objectives and control practices with more detailed ITIL guidance.
8. Measure results, establish a scorecard mechanism for measuring current performance, and monitor the results of new improvements taking into account, as a minimum, the following key considerations:
   – Will the organisational structures support strategy implementation?
   – Are responsibilities for risk management embedded in the organisation?
   – Do infrastructures exist that will facilitate and support the creation and sharing of vital business information?
   – Have strategies and goals been communicated effectively to everyone who needs to know within the organisation?
   COBIT's management guidelines (goals and metrics) can form the basis of a scorecard.
9. Repeat steps 2 through 7 on a regular basis.

Avoiding Pitfalls

There are also some obvious, but pragmatic, rules that management ought to follow to avoid pitfalls:

- Treat the implementation initiative as a project activity with a series of phases rather than a 'one-off' step.
- Remember that implementation involves cultural change as well as new processes. Therefore, a key success factor is the enablement and motivation of these changes.
- Make sure there is a clear understanding of the objectives.
- Manage expectations. In most enterprises, achieving successful oversight of IT takes time and is a continuous improvement process.
- Focus first on where it is easiest to make changes and deliver improvements and build from there, one step at a time.
- Obtain top management buy-in and ownership, based on the principles of best managing the IT investment.
- Avoid the initiative becoming perceived as a purely bureaucratic exercise.
- Avoid the unfocused checklist approach.

6. DETAILED MAPPING

As stated previously, the detailed mapping consists of the 'information requirements' of ITIL v3 that were mapped to each COBIT control objective. The structure follows the domains, processes and control objectives of COBIT. Mappings are primarily made to control objectives, not to COBIT processes. A link to the process was made only if the content of ITIL is applicable to the process as either background reading or a general requirement.

The coverage of the mapped information requirements is denoted in six different levels:
- E—The requirements stated in ITIL v3 exceed the requirements of COBIT. Therefore, ITIL v3 should be seen as the primary source for further information and guidance to improve the process or control objective.
- C—The requirements of the control objective are covered by the mapped requirements of the guidance in ITIL v3.
- A+—Many aspects of the control objective are addressed by ITIL v3.
- A—Some aspects of the control objective are addressed by ITIL v3, but the requirements of the control objective are not covered completely.
- A- —A few aspects of the control objective are addressed by ITIL v3.
- N/A—There is no match between the requirements of COBIT and ITIL v3.

Each COBIT control objective number and title is listed in tables, as shown in the example in **figure 11**.

Figure 11—Example of Detailed Mapping of COBIT With ITIL v3

Control objective example	ITIL v3 Coverage
Control objective number and title	E, C, A+, A, A- or N/A

Legend:
(E) Exceeded
(C) Complete coverage
(A+) Many aspects addressed
(A) Some aspects addressed
(A-) A few aspects addressed
(N/A) Not addressed

The description of the COBIT control objective is provided to give an overview of the aim of the specific part of COBIT. An abstract of the information requirement mapped to the control objective is provided in the ITIL column in **figure 12**. The abstract is focused on the requirement of the specific COBIT control objective and does not contain all requirements of the clause referenced. There is also a reference to the clause of the standard provided in brackets.

Note: Mapping cannot always be one-to-one because the COBIT control objectives operate at a higher level, and the detail of ITIL v3 is much closer to the level of detail of the COBIT control practices.[10]

OVERVIEW

ITIL v3 is outline numbered, broken into 17 families and multiple controls per family. Controls have a reference statement, expanded guidance and control enhancements for environments where the risk suggests a more controlled environment. References provided are at the level of detail of the reference statement.

[10] ITGI, *COBIT® Control Practices: Guidance to Achieve Control Objectives for Successful IT Governance, 2nd Edition*, USA, 2007

Figure 8 on page 20 gives a qualitative overview of the coverage.

Figure 12—Detailed Mapping (COBIT to ITIL)

COBIT		ITIL	Coverage
Control Objective	**Name**		
Framework	Asset types could be compared to resources on framework level	SS App B1 Description of asset types ST App A Description of asset types	N/A
	AI framework level	SD 9 Challenges, critical success factors and risks ST 1 Introduction ST 3 Service transition principles	
	DS framework level	SO 1 Introduction SO 2.4 Service operation fundamentals SO 3 Service operation principles	
PO1	Define a strategic IT plan	SS 1 Introduction SS 2 Service management as a practice SS 3 Service strategy principles SS 3.5 Service strategy fundamentals SS 4 Service strategy SS 5 Service economics SS 6 Strategy and organisation SS 7 Strategy, tactics and operations SS 8 Technology and strategy SS 9 Challenges, critical success factors and risks	A+
PO1.1	IT value management	SS 2.2 What are services? SS 3.1 Value creation SS 3.4 Service structures SS 4.4 Prepare for execution SS 5.1 Financial management SS 5.2 Return on investment SS 5.3 Service portfolio management SS 5.4 Service portfolio management methods	C
PO1.2	Business-IT alignment	SS 2.1 What is service management? SS 2.3 The business process SS 2.4 Principles of service management	C
PO1.3	Assessment of current capability and performance	SS 4.4 Prepare for execution CSI 5.2 Assessments	C
PO1.4	IT strategic plan	SS 3.3 Service provider types SS 3.5 Service strategy fundamentals SS 4.1 Define the market SS 4.2 Develop the offerings SS 4.3 Develop strategic assets SS 4.4 Prepare for execution SS 5.5 Demand management SS 6.5 Sourcing strategy	C
PO1.5	IT tactical plans	SS 4.4 Prepare for execution SS 7.1 Implementation through the life cycle SS 7.2 Strategy and design SS 7.3 Strategy and transitions SS 7.4 Strategy and operations	C

Figure 12—Detailed Mapping (CobiT to ITIL) (*cont.*)

CobiT		ITIL	Coverage
Control Objective	Name		
PO1.6	IT portfolio management	SS 2.5 The service lifecycle SS 3.4 Service structures SS 4.2 Develop the offerings SS 4.3 Develop strategic assets SS 5.3 Service portfolio management SS 5.4 Service portfolio management methods SS 5.5 Demand management SD 3.4 Identifying and documenting business requirements and drivers SD 3.6.1 Designing service solutions SD 3.6.2 Designing supporting systems, especially the service portfolio	A
PO2	Define the information architecture		A-
PO2.1	Enterprise information architecture model	SD 3.6 Design aspects SD 3.6.3 Designing technology architectures SD 3.9 Service-oriented architecture SD 3.10 Business service management SD 5.2 Data and information management ST 4.7 Knowledge management (weak coverage)	A
PO2.2	Enterprise data dictionary and data syntax rules	SD 5.2 Data and information management SD 7 Technology considerations	A
PO2.3	Data classification scheme	SD 5.2 Data and information management	A
PO2.4	Integrity management	SD 5.2 Data and information management ST 4.7 Knowledge management (weak coverage)	A
PO3	Determine technological direction		A-
PO3.1	Technological direction planning	SS 8 Technology and strategy	A
PO3.2	Technological infrastructure plan	SD 3.6.3 Designing technology architectures	A
PO3.3	Monitor future trends and regulations	SS 2.4 Principles of service management SD 4.3.5.7 Modelling and trending	A
PO3.4	Technology standards		N/A
PO3.5	IT architecture board		N/A
PO4	Define the IT processes, organisation and relationships	SD 2.3 Functions and processes across lifecycle SD 6 Organising for service design ST 6 Organising for service transition	A+
PO4.1	IT process framework	SS 2.6 Functions and processes across the lifecycle SS 3.4 Service structures SS 7.1 Implementation through the lifecycle SS 9.1 Complexity SS 9.2 Co-ordination and control SS 9.3 Preserving value SS 9.4 Effectiveness in measurement SD 2.4.2 Scope SD 3.6.3 Designing technology architectures SD 3.6.4 Designing processes SD 3.6.5 Design of measurement systems and metrics SD 4 Service design processes SD 6.1 Functional roles analysis SD 6.2 Activity analysis SD 6.3 Skills and attributes	C

Figure 12—Detailed Mapping (COBIT to ITIL) (*cont.*)			
COBIT			
Control Objective	**Name**	**ITIL**	**Coverage**
PO4.1 *(cont)*	IT process framework *(cont)*	SD 6.4 Roles and responsibilities SD 8 Implementing service design SD Appendix C Process documentation templates (example) ST 3.2.7 Establish effective controls and disciplines ST 4 Service transition processes ST 6.1 Generic roles ST 8 Implementing service transition SO 2.3 Functions and processes across the lifecycle SO 4 Service operation processes SO 4.6 Operational activities of processes covered in other lifecycle phases SO 6 Organising for service operation SO 8 Implementing service operation CSI 3.11 Frameworks, models, standards and quality systems CSI 4 Continual service improvement processes CSI 4.1.1 Integration with the rest of the lifecycle stages and service management processes CSI 5.2 Assessments CSI 5.5 The Deming Cycle CSI 8 Implementing continual service improvement	C
PO4.2	IT strategy committee	SD 2.4.2 Scope	A
PO4.3	IT steering committee		N/A
PO4.4	Organisational placement of the IT function	SS 6.1 Organisational development SO 3.2.4 Reactive vs. proactive organisations	A
PO4.5	IT organisational structure	SS 2.6 Functions and processes across the lifecycle SS 6.1 Organisational development SS 6.2 Organisational departmentalisation SS 6.3 Organisational design SS 6.5 Sourcing strategy SS Appendix B2 Product managers SD 6.3 Skills and attributes ST 4.2.6.8 Change advisory board ST 6.2 Organisational context for transitioning a service ST 6.3 Organisation models to support service transition SO 3.1 Functions, groups, teams, departments and divisions SO 3.2 Achieving balance in service operation SO 3.3 Providing service SO 6.1 Functions SO 6.2 Service desk SO 6.3 Technical management SO 6.4 IT operations management SO 6.5 Application management SO 6.7 Service operation organisation structures	C
PO4.6	Establishment of roles and responsibilities	SS 2.6 Functions and processes across the lifecycle SD 6.2 Activity analysis SD 6.4 Roles and responsibilities ST 6.3 Organisation models to support service transition SO 6.6 Service operation roles and responsibilities CSI 6 Organising for continual service improvement	C
PO4.7	Responsibility for IT quality assurance	CSI 6 Organising for continual service improvement	A

Figure 12—Detailed Mapping (CobiT to ITIL) (*cont.*)

CobiT		ITIL	Coverage
Control Objective	Name		
PO4.8	Responsibility for risk, security and compliance	SD 6.4 Roles and responsibilities	A
PO4.9	Data and system ownership	SO 6.3 Technical management	A
PO4.10	Supervision		N/A
PO4.11	Segregation of duties	ST 3.2.13 Assure the quality of the new or changed service SO 5.13 Information security management and service operation	A
PO4.12	IT staffing	SO 6.2 Service desk	A
PO4.13	Key IT personnel		N/A
PO4.14	Contracted staff policies and procedures		N/A
PO4.15	Relationships	SD 4.2.5.9 Develop contracts and relationships	A
PO5	Manage the IT investment	SS 5.1 Financial management SO 4.6.7 Financial management for IT services (as operational activities)	A+
PO5.1	Financial management framework	SS 3.1 Value creation SS 5.1 Financial management SS 5.2 Return on investment SS Appendix A Present value of an annuity	A
PO5.2	Prioritisation within IT budget	SS 5.2 Return on investment SS 5.3 Service portfolio management SS 5.4 Service portfolio management methods	A
PO5.3	IT budgeting	SS 5.2.2 Return on investment SS 5.2.3 Return on investment	C
PO5.4	Cost management	SS 5.1 Financial management (especially 5.1.2.7)	C
PO5.5	Benefit management	SS 2.2 What are services? SS 5.1 Financial management SS 5.2 Return on investment ST 4.4.5.10 Review and close service transition ST 4.4.5.8 Early life support	A
PO6	Communicate management aims and direction		A-
PO6.1	IT policy and control environment	SS 6.4 Organisational culture	A
PO6.2	Enterprise IT risk and internal control framework		N/A
PO6.3	IT policies management		N/A
PO6.4	Policy, standard and procedures rollout		N/A
PO6.5	Communication of IT objectives and direction	ST 5.1 Managing communications and commitment SO 3.6 Communication	A
PO7	Manage IT human resources		A-
PO7.1	Personnel recruitment and retention		N/A
PO7.2	Personnel competencies		N/A
PO7.3	Staffing of roles		N/A
PO7.4	Personnel training	SD 6.3 Skills and attributes	A
PO7.5	Dependence upon individuals		N/A

Figure 12—Detailed Mapping (COBIT to ITIL) (*cont.*)			
COBIT		**ITIL**	**Coverage**
Control Objective	**Name**		
PO7.6	Personnel clearance procedures		N/A
PO7.7	Employee job performance evaluation		N/A
PO7.8	Job change and termination		N/A
PO8	Manage quality		A
PO8.1	Quality management system	SS 7.5 Strategy and improvement ST 4.4.5.3 Build and test	A
PO8.2	IT standards and quality practices	SS 7.5 Strategy and improvement ST 3.2.13 Assure the quality of the new or changed service ST 4.5 Service validation and testing (ITIL is not just focused on service transition, but on ongoing test of the service.) CSI App A Complementary guidance	A
PO8.3	Development and acquisition standards	SS 6.5 Sourcing strategy SD 3.5 Design activities SD 3.6 Design aspects SD 3.9 Service oriented architecture SD 3.11 Service design models SD 5.3 Application management SD 7 Technology considerations ST 3.2.3 Adopt a common framework and standards ST 4.1.4 Policies, principles and basic concepts ST 4.1.5.1 Transition strategy	A
PO8.4	Customer focus	SS 5.5 Demand management SD 4.2.5.4 Collate, measure and improve customer satisfaction ST 3.2.6 Establish and maintain relationships with stakeholders	C
PO8.5	Continuous improvement	SD 4.2.5.7 Conduct service reviews and instigate improvements within an overall systems integration office (SIO) SO 5.14 Improvement of operational activities CSI 1 Introduction CSI 2 Service management as a practice CSI 3 Continual service improvement (CSI) principles CSI 4.1 The seven-step improvement process CSI 4.1.1 Integration with the rest of the lifecycle stages and service management processes CSI 4.4 Return on investment for CSI CSI 4.5 Business questions for CSI CSI 5 CSI methods and techniques CSI 5.1 Methods and techniques CSI 5.5 The Deming Cycle CSI 5.6 CSI and other service management processes CSI 5.6.7 Summary CSI 6 Organizing for CSI CSI 8 Implementing CSI CSI 9 Challenges, critical success factors and risks	E
PO8.6	Quality measurement, monitoring and review	CSI 5.2 Assessments CSI 5.3 Benchmarking CSI 5.4 Measuring and reporting frameworks	C

Figure 12—Detailed Mapping (CobiT to ITIL) (*cont.*)

CobiT		ITIL	Coverage
Control Objective	Name		
PO9	Assess and manage IT risks	SS 9.5 Risks	A
PO9.1	IT risk management framework	SS 9.5 Risks SD 4.5.5.1 Stage 1—Initiation	A
PO9.2	Establishment of risk context	SS 9.5 Risks SD 4.5.5.1 Stage 1—Initiation SD 4.5.5.2 Stage 2—Requirements and strategy	A
PO9.3	Event identification	SS 9.5 Risks SD 4.5.5.2 Stage 2—Requirements and strategy ST 9 Challenges, critical success factors and risks CSI 5.6.3 IT service continuity management	A
PO9.4	Risk assessment	SS 9.5 Risks SD 4.5.5.2 Stage 2—Requirements and strategy SD 8.1 Business impact analysis (not in detail) ST 4.6 Evaluation	A
PO9.5	Risk response	SS 9.5 Risks SD 4.5.5.3 Stage 3—Implementation ST 4.6 Evaluation	A
PO9.6	Maintenance and monitoring of a risk action plan	SS 9.5 Risks SD 4.5.5.4 Stage 4—Ongoing operation	A
PO10	Manage projects		A-
PO10.1	Programme management framework		N/A
PO10.2	Project management framework		N/A
PO10.3	Project management approach	ST 3.2 Policies for service transition	A
PO10.4	Stakeholder commitment	ST 3.2.6 Establish and maintain relationships with stakeholders ST 3.2.12 Ensure early involvement in the service lifecycle	A
PO10.5	Project scope statement	SD 3.4 Identifying and documenting business requirements and drivers SD 3.5 Design activities	A
PO10.6	Project phase initiation		N/A
PO10.7	Integrated project plan	SD App D Design and planning documents and their contents	A
PO10.8	Project resources	ST 3.2.11 Proactively manage resources across service transitions	A
PO10.9	Project risk management		N/A
PO10.10	Project quality plan		N/A
PO10.11	Project change control	ST 3.2.10 Anticipate and manage course corrections	A
PO10.12	Project planning of assurance methods		N/A
PO10.13	Project performance measurement, reporting and monitoring		N/A
PO10.14	Project closure		N/A

Figure 12—Detailed Mapping (COBIT to ITIL) (*cont.*)

COBIT		ITIL	Coverage
Control Objective	Name		
AI1	Identify automated solutions	SD App B Service acceptance criteria (example) ST 2 Service management as a practice SO 6.5 Application management	A+
AI1.1	Definition and maintenance of business functional and technical requirements	SS 7.5 Strategy and improvement SS 8.1 Service automation SD 3.2 Balanced design SD 3.3 Identifying service requirements SD 3.4 Identifying and documenting business requirements and drivers SD 3.5 Design activities SD 3.6.1 Designing service solutions SD 3.6.2 Designing supporting systems, especially the service portfolio SD 3.6.3 Designing technology architectures SD 3.6.4 Designing processes SD 3.6.5 Design of measurement systems and metrics SD 3.8 Design constraints SD 3.9 Service oriented architecture SD 4.3.5.8 Application sizing SD App D Design and planning documents and their contents ST 3.2.5 Align service transition plans with the business needs	C
AI1.2	Risk analysis report	SD 2.4.2 Scope SD 3.6 Design aspects SD 4.5.5.2 Stage 2—Requirements and strategy	A
AI1.3	Feasibility study and formulation of alternative courses of action	SD 3.6.1 Designing service solutions SD 3.7.1 Evaluation of alternative solutions ST 3.2.4 Maximise reuse of established processes and systems	A
AI1.4	Requirements and feasibility decision and approval	SD 3.6.1 Designing service solutions	A
AI2	Acquire and maintain application software		A+
AI2.1	High-level design	SD 3.6.1 Designing service solutions SD 3.6.3 Designing technology architectures	A
AI2.2	Detailed design	SS 8.2 Service interfaces SD 4.2.5.2 Determine, document and agree requirements for new services and produce service level requirements (SLRs) SD 5.3 Application management	A
AI2.3	Application control and auditability		N/A
AI2.4	Application security and availability	SD 3.6.1 Designing service solutions SO 4.4.5.11 Errors detected in the development environment	A
AI2.5	Configuration and implementation of acquired application software		N/A
AI2.6	Major upgrades to existing systems		N/A
AI2.7	Development of application software	SD 3.7.3 Develop the service solution (development is just mentioned, no detailed coverage)	N/A
AI2.8	Software quality assurance		N/A
AI2.9	Applications requirements management	ST 3.2.6 Establish and maintain relationships with stakeholders ST 3.2.10 Anticipate and manage course corrections	A

Figure 12—Detailed Mapping (CobiT to ITIL) (*cont.*)

CobiT		ITIL	Coverage
Control Objective	**Name**		
AI2.10	Application software maintenance		N/A
AI3	Acquire and maintain technology infrastructure		A
AI3.1	Technological infrastructure acquisition plan	SD 3.6.3 Designing technology architectures	A
AI3.2	Infrastructure resource protection and availability	SD 4.6.5.1 Security controls SO 5.4 Server management and support	A
AI3.3	Infrastructure maintenance	SO 5.4 Server management and support SO 5.5 Network management SO 5.7 Database administration SO 5.8 Directory services management SO 5.9 Desktop support SO 5.10 Middleware management SO 5.11 Internet/web management	C
AI3.4	Feasibility test environment	ST 4.4.5.1 Planning ST 4.4.5.2 Preparation for build, test and deployment ST 4.4.5.3 Build and test ST 4.5.5.7 Test clean-up and closure ST 4.5.7 Information management	A
AI4	Enable operation and use	ST 2 Service management as a practice CSI 5.6.6 Knowledge management	A+
AI4.1	Planning for operational solutions	SD 3.6.1 Designing service solutions ST 3.2.5 Align service transition plans with the business needs ST 3.2.9 Plan release and deployment packages ST 4.4.5.1 Planning ST 4.4.5.2 Preparation for build, test and deployment ST 4.4.5.5 Plan and prepare for deployment	C
AI4.2	Knowledge transfer to business management	ST 3.2.5 Align service transition plans with the business needs ST 4.7 Knowledge management	A
AI4.3	Knowledge transfer to end users	ST 3.2.8 Provide systems for knowledge transfer and decision support ST 4.4.5.8 Early life support ST 4.7 Knowledge management	C
AI4.4	Knowledge transfer to operations and support staff	ST 3.2.8 Provide systems for knowledge transfer and decision support ST 4.4.5.5 Plan and prepare for deployment ST 4.7 Knowledge management SO 3.7 Documentation SO 4.4.5.11 Errors detected in the development environment SO 4.6.6 Knowledge management (as operational activities)	C
AI5	Procure IT resources		A+
AI5.1	Procurement control	SD 3.7.2 Procurement of the preferred solution	A
AI5.2	Supplier contract management	SD 4.2.5.9 Develop contracts and relationships SD 4.7.5.3 Establishing new suppliers and contracts	A
AI5.3	Supplier selection	SD 3.7.1 Evaluation of alternative solutions SD 4.7.5.3 Establishing new suppliers and contracts SD App I Example contents of a statement of requirement (SoR) and/or invitation to tender (ITT)	C
AI5.4	Resources acquisition	SD 3.7.2 Procurement of the preferred solution	C

Figure 12—Detailed Mapping (COBIT to ITIL) (*cont.*)			
COBIT			
Control Objective	**Name**	**ITIL**	**Coverage**
AI6	Manage changes	ST 2 Service management as a practice ST 4.2 Change management ST 4.2.6.8 Change advisory board ST 5.1 Managing communications and commitment ST 5.2 Managing organisation and stakeholder change ST 5.3 Stakeholder management SO 4.3 Request fulfilment CSI 5.6.5 Change, release and deployment management	C
AI6.1	Change standards and procedures	SD 3.2 Balanced design SD 3.7 The subsequent design activities ST 3.2 Policies for service transition ST 3.2.1 Define and implement a formal policy for service transition ST 3.2.2 Implement all changes to services through service transition ST 3.2.7 Establish effective controls and disciplines ST 4.1 Transition planning and support ST 4.1.4 Policies, principles and basic concepts ST 4.2 Change management ST 4.2.6.1 Normal change procedure ST 5 Service transition common operation activities ST 6 Organising for service transition ST 6.3 Organisation models to support service transition ST 6.4 Service transition relationship with other lifecycle stages SO 4.6.1 Change management (as operational activities)	E
AI6.2	Impact assessment, prioritisation and authorisation	ST 4.2.6.2 Create and record requests for change ST 4.2.6.3 Review the request for change ST 4.2.6.4 Assess and evaluate the change ST 4.2.6.5 Authorising the change ST 4.2.6.6 Co-ordinating change implementation ST 4.2.6.8 Change advisory board ST 4.6 Evaluation SO 4.3.5.1 Menu selection SO 4.3.5.2 Financial approval SO 4.3.5.3 Other approval	C
AI6.3	Emergency changes	ST 4.2.6.9 Emergency changes	C
AI6.4	Change status tracking and reporting	ST 3.2.13 Assure the quality of the new or changed service ST 3.2.14 Proactively improve quality during service transition ST 4.1.5.3 Planning and co-ordinating service transition ST 4.1.6 Provide transition process support	C
AI6.5	Change closure and documentation	ST 4.2.6.4 Assess and evaluate the change ST 4.2.6.7 Review and close change record ST 4.4.5.10 Review and close service transition ST 4.4.5.9 Review and close a deployment SO 4.3.5.5 Closure	C
AI7	Install and accredit solutions and changes	ST 4.4 Release and deployment management ST 4.4.5.1 Planning ST 4.5 Service validation and testing (ITIL is not just focused on ST, but on ongoing test of the service.) SO 4.6.3 Release and deployment management (as operational activities) CSI 5.6.5 Change, release and deployment management	C
AI7.1	Training	ST 4.4.5.2 Preparation for build, test and deployment	C

Figure 12—Detailed Mapping (CobiT to ITIL) (*cont.*)

CobiT		ITIL	Coverage
Control Objective	Name		
AI7.2	Test plan	ST 4.5.5.1 Validation and test management ST 4.5.5.2 Plan and design test ST 4.5.5.3 Verify test plan and test design ST 4.5.5.4 Prepare test environment	C
AI7.3	Implementation plan	ST 3.2.9 Plan release and deployment packages ST 4.1.5.2 Preparation for service transition ST 4.4.5.2 Preparation for build, test and deployment ST 4.4.5.3 Build and test ST 4.4.5.4 Service testing and pilots ST 4.4.5.5 Plan and prepare for deployment	C
AI7.4	Test environment	ST 3.2.14 Proactively improve quality during service transition ST 4.4.5.2 Preparation for build, test and deployment ST 4.4.5.3 Build and test ST 4.4.5.4 Service testing and pilots	A
AI7.5	System and data conversion		N/A
AI7.6	Testing of changes	ST 3.2.14 Proactively improve quality during service transition ST 4.4.5.4 Service testing and pilots ST 4.5.5.5 Perform tests ST 4.5.5.6 Evaluate exit criteria and report	A
AI7.7	Final acceptance test	ST 4.4.5.4 Service testing and pilots ST 4.5.5.5 Perform tests ST 4.5.5.6 Evaluate exit criteria and report	A
AI7.8	Promotion to production	ST 4.4.5.5 Plan and prepare for deployment ST 4.4.5.6 Perform transfer, deployment and retirement SO 4.3.5.4 Fulfilment	C
AI7.9	Post-implementation review	ST 3.2.13 Assure the quality of the new or changed service ST 4.1.5.3 Planning and co-ordinating service transition ST 4.4.5.10 Review and close service transition ST 4.4.5.7 Verify deployment ST 4.4.5.9 Review and close a deployment ST 4.6 Evaluation SO 4.3.5.5 Closure	C
DS1	Define and manage service levels	SS 2.2 What are services? SS 3.4 Service structures SS 5.3 Service portfolio management SS 8.1 Service automation SD 1 Introduction SD 2 Service management as a practice SD 2.1 What is service management? SD 2.2 What are services? SD 2.4 Service design fundamentals SD 4.2 Service level management SD 5 Service design technology-related activities SD 5.1 Requirements engineering SD 5.2 Data and information management SD 8.2 Service level requirements SD 8.3 Risks to the services and processes SD 8.4 Implementing service design SD App A The service design package SD App B Service acceptance criteria (example) SD App G Example service catalogue	C

Figure 12—Detailed Mapping (COBIT to ITIL) (*cont.*)			
COBIT			
Control Objective	**Name**	**ITIL**	**Coverage**
DS1 (*cont.*)	Define and manage service levels (*cont.*)	ST 2 Service management as a practice SO 2.1 What is service management? SO 2.2 What are services? SO 3.4 Operation staff involvement in service design and service transition CSI 1 Introduction CSI 4.6 Service level management	C
DS1.1	Service level management framework	SS 2.6 Functions and processes across the lifecycle SS 4.3 Develop strategic assets SS 4.4 Prepare for execution SS 7.2 Strategy and design SS 7.3 Strategy and transitions SS 7.5 Strategy and improvement SD 4.2.5.1 Designing SLA frameworks SD 4.2.5.9 Develop contracts and relationships	E
DS1.2	Definition of services	SS 4.2 Develop the offerings SS 4.3 Develop strategic assets SS 5.4 Service portfolio management mtehods SS 5.5 Demand management SS 7.2 Strategy and design SS 7.3 Strategy and transitions SS 7.4 Strategy and operations SS 7.5 Strategy and improvement SS 8.2 Service interfaces SD 3 Service design principles SD 3.1 Goals SD 3.2 Balanced design SD 3.4 Identifying and documenting business requirements and drivers SD 3.5 Design activities SD 3.6 Design aspects SD 4.1 Service catalogue management	E
DS1.3	Service level agreements	SD 4.2.5.2 Determine, document and agree requirements for new services and produce SLR SD App F Sample SLA and operating level agreement (OLA)	E
DS1.4	Operating level agreements	SD 4.2.5.5 Review and revise underpinning agreements and service scope SD App F Sample SLA and OLA	E
DS1.5	Monitoring and reporting of service level achievements	SS 5.3 Service portfolio management SD 4.2.5.3 Monitor service performance against SLA SD 4.2.5.6 Produce service reports SD 4.2.5.7 Conduct service reviews and instigate improvements within an overall SIO SD 4.2.5.10 Complaints and compliments SD 4.3.8 Information management CSI 4.2 Service reporting CSI 4.3 Service measurement	C
DS1.6	Review of service level agreements and contracts	SD 4.2.5.4 Collate, measure and improve customer satisfaction SD 4.2.5.5 Review and revise underpinning agreements and service scope SD 4.2.5.8 Review and revise SLAs, service scope and underpinning agreements	C
DS2	Manage third-party services	SS 6.5 Sourcing strategy SD 4.2.5.9 Develop contracts and relationships SD 4.7 Supplier management	A+

Figure 12—Detailed Mapping (CobiT to ITIL) (*cont.*)

CobiT		ITIL	Coverage
Control Objective	**Name**		
DS2.1	Identification of all supplier relationships	SS 7.3 Strategy and transitions SD 4.7.5.1 Evaluation of new suppliers and contracts SD 4.7.5.2 Supplier categorisation and maintenance of the supplier and contracts database (SCD)	A
DS2.2	Supplier relationship management	SD 4.2.5.9 Develop contracts and relationships SD 4.7.5.2 Supplier categorisation and maintenance of the SCD SD 4.7.5.4 Supplier and contract management and performance SD 4.7.5.5 Contract renewal and/or termination	A
DS2.3	Supplier risk management	SD 4.7.5.3 Establishing new suppliers and contracts SD 4.7.5.5 Contract renewal and/or termination	A
DS2.4	Supplier performance monitoring	SD 4.7.5.4 Supplier and contract management and performance	A
DS3	Manage performance and capacity	SD 4.3 Capacity management SO 4.1 Event management SO 4.6.4 Capacity management (as operational activities) SO 5.1 Monitoring and control (performance monitoring)	C
DS3.1	Performance and capacity planning	SD 4.3.5.1 Business capacity management SD App J The typical contents of a capacity plan CSI 5.6.2 Capacity management	C
DS3.2	Current performance and capacity	SD 4.3.5.2 Service capacity management SD 4.3.5.3 Component capacity management SO 4.1.5.2 Event notification SO 4.1.5.3 Event detection SO 5.4 Server management and support CSI 4.3 Service measurement	C
DS3.3	Future performance and capacity	SD 4.3.5.1 Business capacity management SD 4.3.5.2 Service capacity management SD 4.3.5.3 Component capacity management SD 4.3.5.7 Modelling and trending SD 4.3.8 Information management	C
DS3.4	IT resources availability	SD 4.3.5.3 Component capacity management SD 4.3.5.4 The underpinning activities of capacity management SD 4.4 Availability management SD 4.4.5.1 The reactive activities of availability management SD 4.4.5.2 The proactive activities of availability management SO 4.6.5 Availability management (as operational activities) CSI 5.6.1 Availability management	C
DS3.5	Monitoring and reporting	SD 4.3.5.4 The underpinning activities of capacity management SD 4.3.5.5 Threshold management and control SD 4.3.5.6 Demand management SD 4.4.5.1 The reactive activities of availability management	C
DS4	Ensure continuous service	SO 4.6.8 IT service continuity management	A+
DS4.1	IT continuity framework	SD 4.5 IT service continuity management SD 4.5.5.1 Stage 1—Initiation CSI 5.6.3 IT service continuity management	A
DS4.2	IT continuity plans	SD 4.5.5.2 Stage 2—Requirements and strategy SD 4.5.5.3 Stage 3—Implementation SD App K The typical contents of a recovery plan	C
DS4.3	Critical IT resources	SD 4.4.5.2 The proactive activities of availability management SD 4.5.5.4 Stage 4—Ongoing operation	A

Figure 12—Detailed Mapping (COBIT to ITIL) (*cont.*)

COBIT		ITIL	Coverage
Control Objective	Name		
DS4.4	Maintenance of the IT continuity plan	SD 4.5.5.4 Stage 4—Ongoing operation	C
DS4.5	Testing of the IT continuity plan	SD 4.5.5.3 Stage 3—Implementation SD 4.5.5.4 Stage 4—Ongoing operation	C
DS4.6	IT continuity plan training	SD 4.5.5.3 Stage 3—Implementation SD 4.5.5.4 Stage 4—Ongoing operation	C
DS4.7	Distribution of the IT continuity plan	SD 4.5.5.3 Stage 3—Implementation SD 4.5.5.4 Stage 4—Ongoing operation	C
DS4.8	IT services recovery and resumption	SD 4.4.5.2 The proactive activities of availability management SD 4.5.5.4 Stage 4—Ongoing operation	C
DS4.9	Offsite backup storage	SD 4.5.5.2 Stage 2—Requirements and strategy SO 5.2.3 Back up and restore	C
DS4.10	Post-resumption review	SD 4.5.5.3 Stage 3—Implementation (vague match) SD 4.5.5.4 Stage 4—Ongoing operation	A
DS5	Ensure systems security		A
DS5.1	Management of IT security	SD 4.6 Information security management SO 5.13 Information security management and service operation	A
DS5.2	IT security plan	SD 4.6.4 Policies/principles/basic concepts SD 4.6.5.1 Security controls (high-level coverage, not in detail)	A
DS5.3	Identity management	SO 4.5 Access management	A
DS5.4	User account management	SO 4.5 Access management SO 4.5.5.1 Requesting access SO 4.5.5.2 Verification SO 4.5.5.3 Providing rights SO 4.5.5.4 Monitoring identity status SO 4.5.5.5 Logging and tracking access SO 4.5.5.6 Removing or restricting rights	A
DS5.5	Security testing, surveillance and monitoring	SO 4.5.5.6 Removing or restricting rights SO 5.13 Information security management and service operation	A
DS5.6	Security incident definition	SD 4.6.5.1 Security controls (high-level coverage, not in detail) SD 4.6.5.2 Management of security breaches and incidents	C
DS5.7	Protection of security technology	SO 5.4 Server management and support	A
DS5.8	Cryptographic key management		N/A
DS5.9	Malicious software prevention, detection and correction		N/A
DS5.10	Network security	SO 5.5 Network management	A
DS5.11	Exchange of sensitive data		N/A
DS6	Identify and allocate costs	SO 4.6.7 Financial management for IT services (as operational activities)	C
DS6.1	Definition of services	SS 5.1 Financial management SD 4.1 Service catalogue management	C
DS6.2	IT accounting	SS 5.1 Financial management	C
DS6.3	Cost modelling and charging	SS 5.1 Financial management SS 7.2 Strategy and design	C
DS6.4	Cost model maintenance	SS 5.1 Financial management	C

Figure 12—Detailed Mapping (CobiT to ITIL) (*cont.*)

CobiT		ITIL	Coverage
Control Objective	**Name**		
DS7	Educate and train users		N/A
DS7.1	Identification of education and training needs	SO 5.13 Information security management and service operation (vague) SO 5.14 Improvement of operational activities (vague)	A
DS7.2	Delivery of training and education		N/A
DS7.3	Evaluation of training received		N/A
DS8	Manage service desk and incidents	SO 4.1 Event management SO 4.2 Incident management	C
DS8.1	Service desk	SO 4.1 Event management SO 4.2 Incident management SO 6.2 Service desk	C
DS8.2	Registration of customer queries	SO 4.1.5.3 Event detection SO 4.1.5.4 Event filtering SO 4.1.5.5 Significance of events SO 4.1.5.6 Event correlation SO 4.1.5.7 Trigger SO 4.2.5.1 Incident identification SO 4.2.5.2 Incident logging SO 4.2.5.3 Incident categorisation SO 4.2.5.4 Incident prioritisation SO 4.2.5.5 Initial diagnosis SO 4.3.5.1 Menu selection	E
DS8.3	Incident escalation	SO 4.1.5.8 Response selection SO 4.2.5.6 Incident escalation SO 4.2.5.7 Investigation and diagnosis SO 4.2.5.8 Resolution and recovery SO 5.9 Desktop support	C
DS8.4	Incident closure	SO 4.1.5.10 Close event SO 4.2.5.9 Incident closure	C
DS8.5	Reporting and trend analysis	SO 4.1.5.9 Review and actions CSI 4.3 Service measurement (vague)	C
DS9	Manage the configuration	SS 3.2 Service assets ST 4.3 Service asset and configuration management ST 4.3.4.1 Service asset and configuration management policies ST 4.3.4.2 Basic concepts ST 4.3.4.3 Configuration management system ST 4.3.5.1 Asset and configuration management activities SO 4.6.2 Configuration management (as operational activities)	C
DS9.1	Configuration repository and baseline	SS 8.2 Service interfaces ST 4.1.5.2 Prepare for service transition ST 4.3.5.2 Management and planning	C
DS9.2	Identification and maintenance of configuration items	ST 4.1.5.2 Prepare for service transition ST 4.3.5.3 Configuration identification ST 4.3.5.4 Configuration control ST 4.3.5.5 Status accounting and reporting	C
DS9.3	Configuration integrity review	ST 4.3.5.6 Verification and audit SO 5.4 Server management and support SO 7 Technology considerations (especially for licensing, mentioned in SO 7.1.4)	C

Figure 12—Detailed Mapping (COBIT to ITIL) (*cont.*)

COBIT		ITIL	Coverage
Control Objective	Name		
DS10	Manage problems	SO 4.4 Problem management CSI 5.6.4 Problem management	C
DS10.1	Identification and classification of problems	SO 4.4.5.1 Problem detection SO 4.4.5.3 Problem categorisation SO 4.4.5.4 Problem prioritisation SO App C Kepner and Tregoe SO App D Ishikawa diagrams	C
DS10.2	Problem tracking and resolution	SO 4.4.5.2 Problem logging SO 4.4.5.5 Problem investigation and diagnosis SO 4.4.5.6 Workarounds SO 4.4.5.7 Raising a known error record SO 4.4.5.8 Problem resolution	C
DS10.3	Problem closure	SO 4.4.5.9 Problem closure SO 4.4.5.10 Major problem review	C
DS10.4	Integration of configuration, incident and problem management		N/A
DS11	Manage data		A+
DS11.1	Business requirements for data management	SD 5.2 Data and information management	A
DS11.2	Storage and retention arrangements	SD 5.2 Data and information management SO 5.6 Storage and archive	C
DS11.3	Media library management system		N/A
DS11.4	Disposal		N/A
DS11.5	Backup and restoration	SO 5.2.3 Backup and restore	C
DS11.6	Security requirements for data management	SD 5.2 Data and information management	A
DS12	Manage the physical environment	SD App E Environmental architectures and standards ST 3.1 Principles supporting service transition	A
DS12.1	Site selection and layout		N/A
DS12.2	Physical security measures	SO App E Detailed description of facilities management	A
DS12.3	Physical access	SO App E Detailed description of facilities management SO App F Physical access control	A
DS12.4	Protection against environmental factors	SO App E Detailed description of facilities management	C
DS12.5	Physical facilities management	SO 5.12 Facilities and data centre management	C
DS13	Manage operations	SO 2 Service management as a practice SO 4.1 Event management SO 5.1 Monitoring and control SO 5.2 IT operations SO 6.4 IT operations management	A+
DS13.1	Operations procedures and instructions	SO 3.7 Documentation SO 5 Common service operation activities SO App B Communication in service operation	C

Figure 12—Detailed Mapping (CobiT to ITIL) (*cont.*)

CobiT		ITIL	Coverage
Control Objective	**Name**		
DS13.2	Job scheduling	SD 4.3.5.5 Threshold management and control SD 4.3.5.6 Demand management SO 5.2.2 Job scheduling SO 5.3 Mainframe management	C
DS13.3	IT infrastructure monitoring	SD 4.3.5.4 The underpinning activities of capacity management SD 4.3.5.5 Threshold management and control SO 4.1 Event management SO 4.1.5.1 Event occurs SO 4.1.5.9 Review and actions SO 5.2.1 Console management/operations bridge	C
DS13.4	Sensitive documents and output devices	SO 5.2.4 Print and output	A
DS13.5	Preventive maintenance for hardware	SO 5.3 Mainframe management SO 5.4 Server management and support	A
ME1	Monitor and evaluate IT performance	SD App H The service management process maturity framework SO 5.1 Monitoring and control CSI 1 Introduction	A+
ME1.1	Monitoring approach	SD 8.5 Measurement of service design ST 4.5.5.1 Validation and test management SO 3.5 Operational health CSI 4.1 The seven-step improvement process CSI 4.1a Step One—Define what you should measure CSI 4.1b Step Two—Define what you can measure CSI 4.1.1 Integration with the rest of the lifecycle stages and service management processes CSI 4.1.2 Metrics and measurement CSI 4.3 Service measurement CSI 4.4 Return on investment for CSI CSI 4.5 Business questions for CSI CSI 5.1 Methods and techniques CSI 5.2 Assessments	C
ME1.2	Definition and collection of monitoring data	SD 4.2.5.10 Complaints and compliments CSI 4.1c Step Three—Gathering data CSI 4.1d Step Four—Processing the data	C
ME1.3	Monitoring method	ST 4.5.5.2 Plan and design test ST 4.5.5.3 Verify test plan and test design ST 4.5.5.4 Prepare test environment CSI 4.1b Step Two—Define what you can measure CSI 4.1f Step Six—Presenting and using the information CSI 5.4 Measuring and reporting frameworks	C
ME1.4	Performance assessment	SD 4.2.5.7 Conduct service reviews and instigate improvements within an overall SIO CSI 3 CSI principles CSI 4.1e Step Five—Analysing the data CSI 5.3 Benchmarking CSI 8 Implementing continual service improvement	C
ME1.5	Board and executive reporting	CSI 4.1f Step Six—Presenting and using the information CSI 4.2 Service reporting	A
ME1.6	Remedial actions	CSI 4.1g Step Seven—Implementing corrective action	C

Figure 12—Detailed Mapping (COBIT to ITIL) (*cont.*)

COBIT		ITIL	Coverage
Control Objective	**Name**		
ME2	Monitor and evaluate internal control		N/A
ME2.1	Monitoring of internal control framework		N/A
ME2.2	Supervisory review		N/A
ME2.3	Control exceptions		N/A
ME2.4	Control self-assessment		N/A
ME2.5	Assurance of internal control		N/A
ME2.6	Internal control at third parties		N/A
ME2.7	Remedial actions		N/A
ME3	Ensure compliance with external requirements		N/A
ME3.1	Identification of external legal, regulatory and contractual compliance requirements		N/A
ME3.2	Optimisation of response to external requirements		N/A
ME3.3	Evaluation of compliance with external requirements		N/A
ME3.4	Positive assurance of compliance		N/A
ME3.5	Integrated reporting		N/A
ME4	Provide IT governance		A-
ME4.1	Establishment of an IT governance framework	CSI 3.10 Governance CSI App A Complementary guidance	A
ME4.2	Strategic alignment	SD 3.10 Business service management	A
ME4.3	Value delivery	SS 3.1 Value creation	A
ME4.4	Resource management		N/A
ME4.5	Risk management	SS 9.5 Risks	A
ME4.6	Performance measurement	SS 4.4 Prepare for execution SS 9.4 Effectiveness in measurement SD 3.6.5 Design of measurement systems and metrics CSI 4.3 Service measurement	A
ME4.7	Independent assurance		N/A
Process controls			
PC1	Process goals and objectives	SD 4.x.1 Purpose/goal/objective ST 4.x.1 Purpose/goal/objective SO 4.x.1 Purpose/goal/objective	A
PC2	Process ownership	CSI 6 Organizing for CSI	A
PC3	Process repeatability	SD 3.6.4 Designing processes SD 7 Technology considerations ST 7 Technology considerations SO 7 Technology considerations	A
	DS framework level	SO 9 Challenges, critical success factors and risks	
	Focused on DS1	SS 8.3 Tools for service strategy	

Figure 12—Detailed Mapping (CobiT to ITIL) (*cont.*)			
CobiT		ITIL	Coverage
Control Objective	Name		
PC4	Roles and responsibilities	SD 6 Organising for service design SD 6.1 Functional roles analysis SD 6.2 Activity analysis ST 4.2.6.8 Change advisory board ST 6 Organising for service transition ST 6.1 Generic roles SO 6 Organising for service operation CSI 6 Organising for continual service improvement	A
PC5	Policy, plans and procedures	SD 7 Technology considerations ST 7 Technology considerations SO 7 Technology considerations CSI 7 Technology considerations	A
PC6	Process performance improvement	SS 8.3 Tools for service strategy (focused on DS1) CSI 3 CSI principles CSI 5 CSI methods and techniques CSI 5.6 CSI and other service management processes CSI 6 Organising for CSI	A
Application controls			
AC1	Source data preparation and authorisation		N/A
AC2	Source data collection and entry		N/A
AC3	Accuracy, completeness and authenticity checks		N/A
AC4	Processing integrity and validity		N/A
AC5	Output review, reconciliation and error handling		N/A
AC6	Transaction authentication and integrity	SO 5.10 Middleware management	A

RESULT

Figure 13 provides the content of **figure 12** in the ITIL structure. Please note that this does not represent a reverse mapping, but a reverse sorting of the table in **figure 12**. In addition, there is no indication of coverage intended for this list; it should help individuals familiar with the ITIL structure navigate to the relevant CobiT control objectives.

Figure 13—Detailed Mapping (ITIL to CobiT)	
Index of ITIL	Linkage to CobiT
Service Strategy	
SS 1 Introduction	PO1 Define a strategic IT plan
SS 2 Service management as a practice	PO1 Define a strategic IT plan
SS 2.1 What is service management?	PO1.2 Business-IT alignment
SS 2.2 What are services?	PO1.1 IT value management PO5.5 Benefit management DS1 Define and manage service levels
SS 2.3 The business process	PO1.2 Business-IT alignment
SS 2.4 Principles of service management	PO1.2 Business-IT alignment PO3.3 Monitoring of future trends and regulations
SS 2.5 The service lifecycle	PO1.6 IT portfolio management

Figure 13—Detailed Mapping (ITIL to COBIT) (*cont.*)	
Index of ITIL	**Linkage to COBIT**
Service Strategy (*cont.*)	
SS 2.6 Functions and processes across the lifecycle	PO4.1 IT process framework PO4.5 IT organisational structure PO4.6 Establishment of roles and responsibilities DS1.1 Service level management framework
SS 3 Service strategy principles	PO1 Define a strategic IT plan
SS 3.1 Value creation	PO1.1 IT value management PO5.1 Financial management framework ME4.3 Value delivery
SS 3.2 Service assets	DS9 Manage the configuration
SS 3.3 Service provider types	PO1.4 IT strategic plan
SS 3.4 Service structures	PO1.1 IT value management PO1.6 IT portfolio management PO4.1 IT process framework DS1 Define and manage service levels
SS 3.5 Service strategy fundamentals	PO1 Define a strategic IT plan PO1.4 IT strategic plan
SS 4 Service strategy	PO1 Define a strategic IT plan
SS 4.1 Define the market	PO1.4 IT strategic plan
SS 4.2 Develop the offerings	PO1.4 IT strategic plan PO1.6 IT portfolio management DS1.2 Definition of services
SS 4.3 Develop strategic assets	PO1.4 IT strategic plan PO1.6 IT portfolio management DS1.1 Service level management framework DS1.2 Definition of services
SS 4.4 Prepare for execution	PO1.1 IT value management PO1.3 Assessment of current capability and performance PO1.4 IT strategic plan PO1.5 IT tactical plans DS1.1 Service level management framework ME4.6 Performance measurement
SS 5 Service economics	PO1 Define a strategic IT plan
SS 5.1 Financial management	PO1.1 IT value management PO5 Manage the IT investment PO5.1 Financial management framework PO5.4 Cost management PO5.5 Benefit management DS6.1 Definition of services DS6.2 IT accounting DS6.3 Cost modelling and charging DS6.4 Cost model maintenance
SS 5.2 Return on investment	PO1.1 IT value management PO5.1 Financial management framework PO5.2 Prioritisation within IT budget PO5.5 Benefit management
SS 5.2.2 Return on investment	PO5.3 IT budgeting
SS 5.2.3 Return on investment	PO5.3 IT budgeting
SS 5.3 Service portfolio management	PO1.1 IT value management PO1.6 IT portfolio management PO5.2 Prioritisation within IT budget DS1 Define and manage service levels DS1.5 Monitoring and reporting of service level achievements

Figure 13—Detailed Mapping (ITIL to CobiT) (*cont.*)	
Index of ITIL	**Linkage to CobiT**
Service Strategy (*cont.*)	
SS 5.4 Service portfolio management methods	PO1.1 IT value management PO1.6 IT portfolio management PO5.2 Prioritisation within IT budget PO1.2 Definition of services
SS 5.5 Demand management	PO1.4 IT strategic plan PO1.6 IT portfolio management PO8.4 Customer focus DS1.2 Definition of services
SS 6 Strategy and organisation	PO1 Define a strategic IT plan
SS 6.1 Organisational development	PO4.4 Organisational placement of the IT function PO4.5 IT organisational structure
SS 6.2 Organisational departmentalisation	PO4.5 IT organisational structure
SS 6.3 Organisational design	PO4.5 IT organisational structure
SS 6.4 Organisational culture	PO6.1 IT policy and control environment
SS 6.5 Sourcing strategy	PO1.4 IT strategic plan PO4.5 IT organisational structure PO8.3 Development and acquisition standards DS2 Manage third-party services
SS 7 Strategy, tactics and operations	PO1 Define a strategic IT plan
SS 7.1 Implementation through the lifecycle	PO1.5 IT tactical plans PO4.1 IT process framework
SS 7.2 Strategy and design	PO1.5 IT tactical plans DS1.1 Service level management framework DS1.2 Definition of services DS6.3 Cost modelling and charging
SS 7.3 Strategy and transitions	PO1.5 IT tactical plans DS1.1 Service level management framework DS1.2 Definition of services DS2.1 Identification of all supplier relationships
SS 7.4 Strategy and operations	PO1.5 IT tactical plans DS1.2 Definition of services
SS 7.5 Strategy and improvement	PO8.1 Quality management system PO8.2 IT standards and quality practices AI1.1 Definition and maintenance of business functional and technical requirements DS1.1 Service level management framework DS1.2 Definition of services
SS 8 Technology and strategy	PO1 Define a strategic IT plan PO3.1 Technological direction planning
SS 8.1 Service automation	AI1.1 Definition and maintenance of business functional and technical requirements DS1 Define and manage service levels
SS 8.2 Service interfaces	AI2.2 Detailed design DS1.2 Definition of services DS9.1 Configuration repository and baseline
SS 8.3 Tools for service strategy (focused on DS1)	PC3 Process repeatability PC6 Process performance improvement
SS 9 Challenges, critical success factors and risks	PO1 Define a strategic IT plan
SS 9.1 Complexity	PO4.1 IT process framework
SS 9.2 Co-ordination and control	PO4.1 IT process framework

Figure 13—Detailed Mapping (ITIL to COBIT) (*cont.*)	
Index of ITIL	**Linkage to COBIT**
Service Strategy (*cont.*)	
SS 9.3 Preserving value	PO4.1 IT process framework
SS 9.4 Effectiveness in measurement	PO4.1 IT process framework ME4.6 Performance measurement
SS 9.5 Risks	PO9 Assess and manage IT risks PO9.1 IT risk management framework PO9.2 Establishment of risk context PO9.3 Event identification PO9.4 Risk assessment PO9.5 Risk response PO9.6 Maintenance and monitoring of a risk action plan ME4.5 Risk management
SS App A Present value of an annuity	PO5.1 Financial management framework
SS App B1 Description of asset types	Asset types could be compared to resources on framework level
SS App B2 Product managers	PO4.5 IT Organisational structure
Service Design	
SD 1 Introduction	DS1 Define and manage service levels
SD 2 Service management as a practice	DS1 Define and manage service levels
SD 2.1 What is service management?	DS1 Define and manage service levels
SD 2.2 What are services?	DS1 Define and manage service levels
SD 2.3 Functions and processes across lifecycle	PO4 Define the IT processes, organisation and relationships
SD 2.4 Service design fundamentals	DS1 Define and manage service levels
SD 2.4.2 Scope	PO4.1 IT process framework PO4.2 IT strategy committee AI1.2 Risk analysis report
SD 3 Service design principles	DS1.2 Definition of services
SD 3.1 Goals	DS1.2 Definition of services
SD 3.2 Balanced design	AI1.1 Definition and maintenance of business functional and technical requirements AI6.1 Change standards and procedures DS1.2 Definition of services
SD 3.3 Identifying service requirements	AI1.1 Definition and maintenance of business functional and technical requirements
SD 3.4 Identifying and documenting business requirements and drivers	PO1.6 IT portfolio management PO10.5 Project scope statement AI1.1 Definition and maintenance of business functional and technical requirements DS1.2 Definition of services
SD 3.5 Design activities	PO8.3 Development and acquisition standards PO10.5 Project scope statement AI1.1 Definition and maintenance of business functional and technical requirements DS1.2 Definition of services
SD 3.6 Design aspects	PO2.1 Enterprise information architecture model PO8.3 Development and acquisition standards AI1.2 Risk analysis report DS1.2 Definition of services

Figure 13—Detailed Mapping (ITIL to CobiT) (*cont.*)	
Index of ITIL	**Linkage to CobiT**
Service Design (*cont.*)	
SD 3.6.1 Designing service solutions	PO1.6 IT portfolio management AI1.1 Definition and maintenance of business functional and technical requirements AI1.3 Feasibility study and formulation of alternative courses of action AI1.4 Requirements and feasibility decision and approval AI2.1 High-level design AI2.4 Application security and availability AI4.1 Planning for operational solutions
SD 3.6.2 Designing supporting systems, especially the service portfolio	PO1.6 IT portfolio management AI1.1 Definition and maintenance of business functional and technical requirements
SD 3.6.3 Designing technology architectures	PO2.1 Enterprise information architecture model PO3.2 Technological infrastructure plan PO4.1 IT process framework AI1.1 Definition and maintenance of business functional and technical requirements AI2.1 High-level design AI3.1 Technological infrastructure acquisition plan
SD 3.6.4 Designing processes	PO4.1 IT process framework AI1.1 Definition and maintenance of business functional and technical requirements PC3 Process repeatability
SD 3.6.5 Design of measurement systems and metrics	PO4.1 IT process framework AI1.1 Definition and maintenance of business functional and technical requirements ME4.6 Performance measurement
SD 3.7 The subsequent design activities	AI6.1 Change standards and procedures
SD 3.7.1 Evaluation of alternative solutions	AI1.3 Feasibility study and formulation of alternative courses of action AI5.3 Supplier selection
SD 3.7.2 Procurement of the preferred solution	AI5.1 Procurement control AI5.4 IT resources acquisition
SD 3.7.3 Develop the service solution (development is just mentioned, no detailed coverage)	AI2.7 Development of application software
SD 3.8 Design constraints	AI1.1 Definition and maintenance of business functional and technical requirements
SD 3.9 Service-oriented architecture	PO2.1 Enterprise information architecture model PO8.3 Development and acquisition standards AI1.1 Definition and maintenance of business functional and technical requirements
SD 3.10 Business service management	PO2.1 Enterprise information architecture model ME4.2 Strategic alignment
SD 3.11 Service design models	PO8.3 Development and acquisition standards
SD 4 Service design processes	PO4.1 IT process framework
SD 4.x.1 Purpose/goal/objective	PC1 Process goals and objectives
SD 4.1 Service catalogue management	DS1.2 Definition of services DS6.1 Definition of services
SD 4.2 Service level management	DS1 Define and manage service levels
SD 4.2.5.1 Designing SLA frameworks	DS1.1 Service level management framework
SD 4.2.5.2 Determine, document and agree requirements for new services and produce SLR	AI2.2 Detailed design DS1.3 Service level agreements

Figure 13—Detailed Mapping (ITIL to COBIT) (*cont.*)	
Index of ITIL	**Linkage to COBIT**
Service Design (*cont.*)	
SD 4.2.5.3 Monitor service performance against SLA	DS1.5 Monitoring and reporting of service level achievements
SD 4.2.5.4 Collate, measure and improve customer satisfaction	PO8.4 Customer focus DS1.6 Review of service level agreements and contracts
SD 4.2.5.5 Review and revise underpinning agreements and service scope	DS1.4 operating level agreements DS1.6 Review of service level agreements and contracts
SD 4.2.5.6 Produce service reports	DS1.5 Monitoring and reporting of service level achievements
SD 4.2.5.7 Conduct service reviews and instigate improvements within an overall SIO	PO8.5 Continuous improvement DS1.5 Monitoring and reporting of service level achievements ME1.4 Performance assessment
SD 4.2.5.8 Review and revise SLAs, service scope and underpinning agreements	DS1.6 Review of service level agreements and contracts
SD 4.2.5.9 Develop contracts and relationships	PO4.15 Relationships AI5.2 Supplier contract management DS1.1 Service level management framework DS2 Manage third-party services DS2.2 Supplier relationship management
SD 4.2.5.10 Complaints and compliments	DS1.5 Monitoring and reporting of service level achievements ME1.2 Definition and collection of monitoring data
SD 4.3 Capacity management	DS3 Manage performance and capacity
SD 4.3.5.1 Business capacity management	DS3.1 Performance and capacity planning DS3.3 Future performance and capacity
SD 4.3.5.2 Service capacity management	DS3.2 Current performance and capacity DS3.3 Future performance and capacity
SD 4.3.5.3 Component capacity management	DS3.2 Current performance and capacity DS3.3 Future performance and capacity DS3.4 IT resources availability
SD 4.3.5.4 The underpinning activities of capacity management	DS3.4 IT resources availability DS3.5 Monitoring and reporting DS13.3 IT infrastructure monitoring
SD 4.3.5.5 Threshold management and control	DS3.5 Monitoring and reporting DS13.2 Job scheduling DS13.3 IT infrastructure monitoring
SD 4.3.5.6 Demand management	DS3.5 Monitoring and reporting DS13.2 Job scheduling
SD 4.3.5.7 Modelling and trending	PO3.3 Monitoring of future trends and regulations DS3.3 Future performance and capacity
SD 4.3.5.8 Application sizing	AI1.1 Definition and maintenance of business functional and technical requirements
SD 4.3.8 Information management	DS1.5 Monitoring and reporting of service level achievements DS3.3 Future performance and capacity
SD 4.4 Availability management	DS3.4 IT resources availability
SD 4.4.5.1 The reactive activities of availability management	DS3.4 IT resources availability DS3.5 Monitoring and reporting
SD 4.4.5.2 The proactive activities of availability management	DS3.4 IT resources availability DS4.3 Critical IT resources DS4.8 IT services recovery and resumption
SD 4.5 IT service continuity management	DS4.1 IT continuity framework
SD 4.5.5.1 Stage 1—Initiation	PO9.1 IT risk management framework PO9.2 Establishment of risk context DS4.1 IT continuity framework

Figure 13—Detailed Mapping (ITIL to CobiT) (*cont.*)	
Index of ITIL	**Linkage to CobiT**
Service Design (*cont.*)	
SD 4.5.5.2 Stage 2—Requirements and strategy	PO9.2 Establishment of risk context PO9.3 Event identification PO9.4 Risk assessment AI1.2 Risk analysis report DS4.2 IT continuity plans DS4.9 Offsite backup storage
SD 4.5.5.3 Stage 3—Implementation (vague match)	PO9.5 Risk response DS4.2 IT continuity plans DS4.5 Testing of the IT continuity plan DS4.6 IT continuity plan training DS4.7 Distribution of the IT continuity plan DS4.10 Post-resumption review
SD 4.5.5.4 Stage 4—Ongoing operation	PO9.6 Maintenance and monitoring of a risk action plan DS4.3 Critical IT resources DS4.4 Maintenance of the IT continuity plan DS4.5 Testing of the IT continuity plan DS4.6 IT continuity plan training DS4.7 Distribution of the IT continuity plan DS4.8 IT services recovery and resumption DS4.10 Post-resumption review
SD 4.6 Information security management	DS5.1 Management of IT security
SD 4.6.4 Policies/principles/basic concepts	DS5.2 IT security plan
SD 4.6.5.1 Security controls	AI3.2 Infrastructure resource protection and availability DS5.2 IT security plan DS5.6 Security incident definition
SD 4.6.5.2 Management of security breaches and incidents	DS5.6 Security incident definition
SD 4.7 Supplier management	DS2 Manage third-party services
SD 4.7.5.1 Evaluation of new suppliers and contracts	DS2.1 Identification of all supplier relationships
SD 4.7.5.2 Supplier categorisation and maintenance of the SCD	DS2.1 Identification of all supplier relationships DS2.2 Supplier relationship management
SD 4.7.5.3 Establishing new suppliers and contracts	AI5.2 Supplier contract management AI5.3 Supplier selection DS2.3 Supplier risk management
SD 4.7.5.4 Supplier and contract management and performance	DS2.2 Supplier relationship management DS2.4 Supplier performance monitoring
SD 4.7.5.5 Contract renewal and/or termination	DS2.2 Supplier relationship management DS2.3 Supplier risk management
SD 5 Service design technology-related activities	DS1 Define and manage service levels
SD 5.1 Requirements engineering	DS1 Define and manage service levels
SD 5.2 Data and information management	PO2.1 Enterprise information architecture model PO2.2 Enterprise data dictionary and data syntax rules PO2.3 Data classification scheme PO2.4 Integrity management DS1 Define and manage service levels DS11.1 Business requirements for data management DS11.2 Storage and retention arrangements DS11.6 Security requirements for data management
SD 5.3 Application management	PO8.3 Development and acquisition standards AI2.2 Detailed design
SD 6 Organising for service design	PO4 Define the IT processes, organisation and relationships PC4 Roles and responsibilities

Figure 13—Detailed Mapping (ITIL to COBIT) (*cont.*)	
Index of ITIL	**Linkage to COBIT**
Service Design (*cont.*)	
SD 6.1 Functional roles analysis	PO4.1 IT process framework PC4 Roles and responsibilities
SD 6.2 Activity analysis	PO4.1 IT process framework PO4.6 Establishment of roles and responsibilities PC4 Roles and responsibilities
SD 6.3 Skills and attributes	PO4.1 IT process framework PO4.5 IT organisational structure PO7.4 Personnel training
SD 6.4 Roles and responsibilities	PO4.1 IT process framework PO4.6 Establishment of roles and responsibilities PO4.8 Responsibility for risk, security and compliance
SD 7 Technology considerations	PO2.2 Enterprise data dictionary and data syntax rules PO8.3 Development and acquisition standards PC3 Process repeatability PC5 Policy, plans and procedures
SD 8 Implementing service design	PO4.1 IT process framework
SD 8.1 Business impact analysis (not in detail)	PO9.4 Risk assessment
SD 8.2 Service level requirements	DS1 Define and manage service levels
SD 8.3 Risks to the services and processes	DS1 Define and manage service levels
SD 8.4 Implementing service design	DS1 Define and manage service levels
SD 8.5 Measurement of service design	ME1.1 Monitoring approach
SD 9 Challenges, critical success factors and risks	AI framework level
SD App A The service design package	DS1 Define and manage service levels
SD App B Service acceptance criteria (example)	AI1 Identify automated solutions DS1 Define and manage service levels
SD App C Process documentation templates (example)	PO4.1 IT process framework
SD App D Design and planning documents and their contents	PO10.7 Integrated project plan AI1.1 Definition and maintenance of business functional and technical requirements
SD App E Environmental architectures and standards	DS12 Manage the physical environment
SD App F Sample SLA and OLA	DS1.3 Service level agreements DS1.4 Operating level agreements
SD App G Example service catalogue	DS1 Define and manage service levels
SD App H The service management process maturity framework	ME1 Monitor and evaluate IT performance
SD App I Example contents of a statement of requirement (SoR) and/or invitation to tender (ITT)	AI5.3 Supplier selection
SD App J The typical contents of a capacity plan	DS3.1 Performance and capacity planning
SD App K The typical contents of a recovery plan	DS4.2 IT continuity plans
Service Transition	
ST 1 Introduction	AI framework level
ST 2 Service management as a practice	AI1 Identify automated solutions AI4 Enable operation and use AI6 Manage changes DS1 Define and manage service levels
ST 3 Service transition principles	AI framework level
ST 3.1 Principles supporting service transition	DS12 Manage the physical environment
ST 3.2 Policies for service transition	PO10.3 Project management approach AI6.1 Change standards and procedures

Figure 13—Detailed Mapping (ITIL to CobiT) (*cont.*)	
Index of ITIL	**Linkage to CobiT**
Service Transition (*cont.*)	
ST 3.2.1 Define and implement a formal policy for service transition	AI6.1 Change standards and procedures
ST 3.2.2 Implement all changes to services through service transition	AI6.1 Change standards and procedures
ST 3.2.3 Adopt a common framework and standards	PO8.3 Development and acquisition standards
ST 3.2.4 Maximise re-use of established processes and systems	AI1.3 Feasibility study and formulation of alternative courses of action
ST 3.2.5 Align service transition plans with the business needs	AI1.1 Definition and maintenance of business functional and technical requirements AI4.1 Planning for operational solutions AI4.2 Knowledge transfer to business management
ST 3.2.6 Establish and maintain relationships with stakeholders	PO8.4 Customer focus PO10.4 Stakeholder commitment AI2.9 Applications requirements management
ST 3.2.7 Establish effective controls and disciplines	PO4.1 IT process framework AI6.1 Change standards and procedures
ST 3.2.8 Provide systems for knowledge transfer and decision support	AI4.3 Knowledge transfer to end users AI4.4 Knowledge transfer to operations and support staff
ST 3.2.9 Plan release and deployment packages	AI4.1 Planning for operational solutions AI7.3 Implementation plan
ST 3.2.10 Anticipate and manage course corrections	PO10.11 Project change control AI2.9 Applications requirements management
ST 3.2.11 Proactively manage resources across service transitions	PO10.8 Project resources
ST 3.2.12 Ensure early involvement in the service life cycle	PO10.4 Stakeholder commitment
ST 3.2.13 Assure the quality of the new or changed service	PO4.11 Segregation of duties PO8.2 IT standards and quality practices AI6.4 Change status tracking and reporting AI7.9 Post-implementation review
ST 3.2.14 Proactively improve quality during service transition	AI6.4 Change status tracking and reporting AI7.4 Test environment AI7.6 Testing of changes
ST 4 Service transition processes	PO4.1 IT process framework
ST 4.1 Transition planning and support	AI6.1 Change standards and procedures
ST 4.x.1 Purpose, goals and objectives	PC1 Process goals and objectives
ST 4.1.4 Policies, principles and basic concepts	PO8.3 Development and acquisition standards AI6.1 Change standards and procedures
ST 4.1.5.1 Transition strategy	PO8.3 Development and acquisition standards
ST 4.1.5.2 Prepare for service transition	AI7.3 Implementation plan DS9.1 Configuration repository and baseline DS9.2 Identification and maintenance of configuration items
ST 4.1.5.3 Planning and co-ordinating service transition	AI6.4 Change status tracking and reporting AI7.9 Post-implementation review
ST 4.1.6 Provide transition process support	AI6.4 Change status tracking and reporting
ST 4.2 Change management	AI6 Manage changes AI6.1 Change standards and procedures
ST 4.2.6.1 Normal change procedure	AI6.1 Change standards and procedures
ST 4.2.6.2 Create and record requests for change	AI6.2 Impact assessment, prioritisation and authorisation
ST 4.2.6.3 Review the request for change	AI6.2 Impact assessment, prioritisation and authorisation
ST 4.2.6.4 Assess and evaluate the change	AI6.2 Impact assessment, prioritisation and authorisation AI6.5 Change closure and documentation
ST 4.2.6.5 Authorising the change	AI6.2 Impact assessment, prioritisation and authorisation

Figure 13—Detailed Mapping (ITIL to COBIT) (*cont.*)	
Index of ITIL	**Linkage to COBIT**
Service Transition (*cont.*)	
ST 4.2.6.6 Co-ordinating change implementation	AI6.2 Impact assessment, prioritisation and authorisation
ST 4.2.6.7 Review and close change record	AI6.5 Change closure and documentation
ST 4.2.6.8 Change advisory board	PO4.5 IT organisational structure AI6 Manage changes AI6.2 Impact assessment, prioritisation and authorisation PC4 Roles and responsibilities
ST 4.2.6.9 Emergency changes	AI6.3 Emergency changes
ST 4.3 Service asset and configuration management	DS9 Manage the configuration
ST 4.3.4.1 Service asset and configuration management policies	DS9 Manage the configuration
ST 4.3.4.2 Basic concepts	DS9 Manage the configuration
ST 4.3.4.3 Configuration management system	DS9 Manage the configuration
ST 4.3.5.1 Asset and configuration management activities	DS9 Manage the configuration
ST 4.3.5.2 Management and planning	DS9.1 Configuration repository and baseline
ST 4.3.5.3 Configuration identification	DS9.2 Identification and maintenance of configuration items
ST 4.3.5.4 Configuration control	DS9.2 Identification and maintenance of configuration items
ST 4.3.5.5 Status accounting and reporting	DS9.2 Identification and maintenance of configuration items
ST 4.3.5.6 Verification and audit	DS9.3 Configuration integrity review
ST 4.4 Release and deployment management	AI7 Install and accredit solutions and changes
ST 4.4.5.1 Planning	AI3.4 Feasibility test environment AI4.1 Planning for operational solutions AI7 Install and accredit solutions and changes
ST 4.4.5.2 Preparation for build, test and deployment	AI3.4 Feasibility test environment AI4.1 Planning for operational solutions AI7.1 Training AI7.3 Implementation plan AI7.4 Test environment
ST 4.4.5.3 Build and test	PO8.1 Quality management system AI3.4 Feasibility test environment AI7.3 Implementation plan AI7.4 Test environment
ST 4.4.5.4 Service testing and pilots	AI7.3 Implementation plan AI7.4 Test environment AI7.6 Testing of changes AI7.7 Final acceptance test
ST 4.4.5.5 Plan and prepare for deployment	AI4.1 Planning for operational solutions AI4.4 Knowledge transfer to operations and support staff AI7.3 Implementation plan AI7.8 Promotion to production
ST 4.4.5.6 Perform transfer, deployment and retirement	AI7.8 Promotion to production
ST 4.4.5.7 Verify deployment	AI7.9 Post-implementation review
ST 4.4.5.8 Early life support	PO5.5 Benefit management AI4.3 Knowledge transfer to end users
ST 4.4.5.9 Review and close a deployment	AI6.5 Change closure and documentation AI7.9 Post-implementation review
ST 4.4.5.10 Review and close service transition	PO5.5 Benefit management AI6.5 Change closure and documentation AI7.9 Post-implementation review

Figure 13—Detailed Mapping (ITIL to CobiT) (*cont.*)	
Index of ITIL	**Linkage to CobiT**
Service Transition (*cont.*)	
ST 4.5 Service validation and testing (ITIL is not focused just on service transition, but on ongoing test of the service.)	PO8.2 IT standards and quality practices AI7 Install and accredit solutions and changes
ST 4.5.5.1 Validation and test management	AI7.2 Test plan ME1.1 Monitoring approach
ST 4.5.5.2 Plan and design test	AI7.2 Test plan ME1.3 Monitoring method
ST 4.5.5.3 Verify test plan and test design	AI7.2 Test plan ME1.3 Monitoring method
ST 4.5.5.4 Prepare test environment	AI7.2 Test plan ME1.3 Monitoring method
ST 4.5.5.5 Perform tests	AI7.6 Testing of changes AI7.7 Final acceptance test
ST 4.5.5.6 Evaluate exit criteria and report	AI7.6 Testing of changes AI7.7 Final acceptance test
ST 4.5.5.7 Test clean-up and closure	AI3.4 Feasibility test environment
ST 4.5.7 Information management	AI3.4 Feasibility test environment
ST 4.6 Evaluation	PO9.4 Risk assessment PO9.5 Risk response AI6.2 Impact assessment, prioritisation and authorisation AI7.9 Post-implementation review
ST 4.7 Knowledge management	PO2.1 Enterprise information architecture model PO2.4 Integrity management AI4.2 Knowledge transfer to business management AI4.3 Knowledge transfer to end users AI4.4 Knowledge transfer to operations and support staff
ST 5 Service transition common operation activities	AI6.1 Change standards and procedures
ST 5.1 Managing communications and commitment	PO6.5 Communication of IT objectives and direction AI6 Manage changes
ST 5.2 Managing organisation and stakeholder change	AI6 Manage changes
ST 5.3 Stakeholder management	AI6 Manage changes
ST 6 Organising for service transition	PO4 Define the IT processes, organisation and relationships AI6.1 Change standards and procedures PC4 Roles and responsibilities
ST 6.1 Generic roles	PO4.1 IT process framework PC4 Roles and responsibilities
ST 6.2 Organisational context for transitioning a service	PO4.5 IT organisational structure
ST 6.3 Organisation models to support service transition	PO4.5 IT organisational structure PO4.6 Establishment of roles and responsibilities AI6.1 Change standards and procedures
ST 6.4 Service transition relationship with other lifecycle stages	AI6.1 Change standards and procedures
ST 7 Technology considerations	PC3 Process repeatability PC5 Policy, plans and procedures
ST 8 Implementing service transition	PO4.1 IT process framework
ST 9 Challenges, critical success factors and risks	PO9.3 Event identification
ST App A Description of asset types	Asset types could be compared to resources on framework level
Service Operations	
SO 1 Introduction	DS framework level
SO 2 Service management as a practice	DS13 Manage operations

Figure 13—Detailed Mapping (ITIL to COBIT) (*cont.*)	
Index of ITIL	**Linkage to COBIT**
Service Operations (*cont.*)	
SO 2.1 What is service management?	DS1 Define and manage service levels
SO 2.2 What are services?	DS1 Define and manage service levels
SO 2.3 Functions and processes across the lifecycle	PO4.1 IT process framework
SO 2.4 Service operation fundamentals	Framework level
SO 3 Service operation principles	Framework level
SO 3.1 Functions, groups, teams, departments and divisions	PO4.5 IT organisational structure
SO 3.2 Achieving balance in service operation	PO4.5 IT organisational structure
SO 3.2.4 Reactive vs. proactive organisations	PO4.4 Organisational placement of the IT function
SO 3.3 Providing service	PO4.5 IT organisational structure
SO 3.4 Operation staff involvement in service design and service transition	DS1 Define and manage service levels
SO 3.5 Operational health	ME1.1 Monitoring approach
SO 3.6 Communication	PO6.5 Communication of IT objectives and direction
SO 3.7 Documentation	AI4.4 Knowledge transfer to operations and support staff DS13.1 Operations procedures and instructions
SO 4 Service operation processes	PO4.1 IT process framework
SO 4.x.1 Purpose/goal/objective	PC1 Process goals and objectives
SO 4.1 Event management	DS3 Manage performance and capacity DS8 Manage service desk and incidents DS8.1 Service desk DS13 Manage operations DS13.3 IT infrastructure monitoring
SO 4.1.5.1 Event occurs	DS13.3 IT infrastructure monitoring
SO 4.1.5.2 Event notification	DS3.2 Current performance and capacity
SO 4.1.5.3 Event detection	DS3.2 Current performance and capacity DS8.2 Registration of customer queries
SO 4.1.5.4 Event filtering	DS8.2 Registration of customer queries
SO 4.1.5.5 Significance of events	DS8.2 Registration of customer queries
SO 4.1.5.6 Event correlation	DS8.2 Registration of customer queries
SO 4.1.5.7 Trigger	DS8.2 Registration of customer queries
SO 4.1.5.8 Response selection	DS8.3 Incident escalation
SO 4.1.5.9 Review and actions	DS8.5 Reporting and trend analysis DS13.3 IT infrastructure monitoring
SO 4.1.5.10 Close event	DS8.4 Incident closure
SO 4.2 Incident management	DS8 Manage service desk and incidents DS8.1 Service desk
SO 4.2.5.1 Incident identification	DS8.2 Registration of customer queries
SO 4.2.5.2 Incident logging	DS8.2 Registration of customer queries
SO 4.2.5.3 Incident categorisation	DS8.2 Registration of customer queries
SO 4.2.5.4 Incident prioritisation	DS8.2 Registration of customer queries
SO 4.2.5.5 Initial diagnosis	DS8.2 Registration of customer queries
SO 4.2.5.6 Incident escalation	DS8.3 Incident escalation
SO 4.2.5.7 Investigation and diagnosis	DS8.3 Incident escalation
SO 4.2.5.8 Resolution and recovery	DS8.3 Incident escalation
SO 4.2.5.9 Incident closure	DS8.4 Incident closure

Figure 13—Detailed Mapping (ITIL to CobiT) (*cont.*)	
Index of ITIL	**Linkage to CobiT**
Service Operations (*cont.*)	
SO 4.3 Request fulfilment	AI6 Manage changes
SO 4.3.5.1 Menu selection	AI6.2 Impact assessment, prioritisation and authorisation DS8.2 Registration of customer queries
SO 4.3.5.2 Financial approval	AI6.2 Impact assessment, prioritisation and authorisation
SO 4.3.5.3 Other approval	AI6.2 Impact assessment, prioritisation and authorisation
SO 4.3.5.4 Fulfilment	AI7.8 Promotion to production
SO 4.3.5.5 Closure	AI6.5 Change closure and documentation AI7.9 Post-implementation review
SO 4.4 Problem management	DS10 Manage problems
SO 4.4.5.1 Problem detection	DS10.1 Identification and classification of problems
SO 4.4.5.2 Problem logging	DS10.2 Problem tracking and resolution
SO 4.4.5.3 Problem categorisation	DS10.1 Identification and classification of problems
SO 4.4.5.4 Problem prioritisation	DS10.1 Identification and classification of problems
SO 4.4.5.5 Problem investigation and diagnosis	DS10.2 Problem tracking and resolution
SO 4.4.5.6 Workarounds	DS10.2 Problem tracking and resolution
SO 4.4.5.7 Raising a known error record	DS10.2 Problem tracking and resolution
SO 4.4.5.8 Problem resolution	DS10.2 Problem tracking and resolution
SO 4.4.5.9 Problem closure	DS10.3 Problem closure
SO 4.4.5.10 Major problem review	DS10.3 Problem closure
SO 4.4.5.11 Errors detected in the development environment	AI2.4 Application security and availability AI4.4 Knowledge transfer to operations and support staff
SO 4.5 Access management	DS5.3 Identity management DS5.4 User account management
SO 4.5.5.1 Requesting access	DS5.4 User account management
SO 4.5.5.2 Verification	DS5.4 User account management
SO 4.5.5.3 Providing rights	DS5.4 User account management
SO 4.5.5.4 Monitoring identity status	DS5.4 User account management
SO 4.5.5.5 Logging and tracking access	DS5.4 User account management
SO 4.5.5.6 Removing or restricting rights	DS5.4 User account management DS5.5 Security testing, surveillance and monitoring
SO 4.6 Operational activities of processes covered in other lifecycle phases	PO4.1 IT process framework
SO 4.6.1 Change management (as operational activities)	AI6.1 Change standards and procedures
SO 4.6.2 Configuration management (as operational activities)	DS9 Manage the configuration
SO 4.6.3 Release and deployment management (as operational activities)	AI7 Install and accredit solutions and changes
SO 4.6.4 Capacity management (as operational activities)	DS3 Manage performance and capacity
SO 4.6.5 Availability management (as operational activities)	DS3.4 IT resources availability
SO 4.6.6 Knowledge management (as operational activities)	AI4.4 Knowledge transfer to operations and support staff
SO 4.6.7 Financial management for IT services (as operational activities)	PO5 Manage the IT investment DS6 Identify and allocate costs
SO 4.6.8 IT aervice continuity management	DS4 Ensure continuous service
SO 5 Common service operation activities	DS13.1 Operations procedures and instructions
SO 5.1 Monitoring and control	DS3 Manage performance and capacity DS13 Manage operations ME1 Monitor and evaluate IT performance

Figure 13—Detailed Mapping (ITIL to COBIT) (*cont.*)	
Index of ITIL	**Linkage to COBIT**
Service Operations (*cont.*)	
SO 5.2 IT operations	DS13 Manage operations
SO 5.2.1 Console management/operations bridge	DS13.3 IT Infrastructure monitoring
SO 5.2.2 Job scheduling	DS13.2 Job scheduling
SO 5.2.3 Back up and restore	DS4.9 Offsite backup storage DS11.5 Backup and restoration
SO 5.2.4 Print and output	DS13.4 Sensitive documents and output devices
SO 5.3 Mainframe management	DS13.2 Job scheduling DS13.5 Preventive maintenance for hardware
SO 5.4 Server management and support	AI3.2 Infrastructure resource protection and availability AI3.3 Infrastructure maintenance DS3.2 Current performance and capacity DS5.7 Protection of security technology DS9.3 Configuration integrity review DS13.5 Preventive maintenance for hardware
SO 5.5 Network management	AI3.3 Infrastructure maintenance DS5.10 Network security
SO 5.6 Storage and archive	DS11.2 Storage and retention arrangements
SO 5.7 Database administration	AI3.3 Infrastructure maintenance
SO 5.8 Directory services management	AI3.3 Infrastructure maintenance
SO 5.9 Desktop support	AI3.3 Infrastructure maintenance DS8.3 Incident escalation
SO 5.10 Middleware management	AI3.3 Infrastructure maintenance AC6 Transaction authentication and integrity
SO 5.11 Internet/web management	AI3.3 Infrastructure maintenance
SO 5.12 Facilities and data centre management	DS12.5 Physical facilities management
SO 5.13 Information security management and service operation (vague)	PO4.11 Segregation of duties DS5.1 Management of IT security DS5.5 Security testing, surveillance and monitoring DS7.1 Identification of education and training needs
SO 5.14 Improvement of operational activities (vague)	PO8.5 Continuous improvement DS7.1 Identification of education and training needs
SO 6 Organising for service operation	PO4.1 IT process framework PC4 Roles and responsibilities
SO 6.1 Functions	PO4.5 IT organisational structure
SO 6.2 Service desk	PO4.5 IT organisational structure PO4.12 IT staffing DS8.1 Service desk
SO 6.3 Technical management	PO4.5 IT organisational structure PO4.9 Data and system ownership
SO 6.4 IT operations management	PO4.5 IT organisational structure DS13 Manage operations
SO 6.5 Application management	PO4.5 IT organisational structure AI1 Identify automated solutions
SO 6.6 Service operation roles and responsibilities	PO4.6 Establishment of roles and responsibilities
SO 6.7 Service operation organisation structures	PO4.5 IT organisational structure
SO 7 Technology considerations (especially for licensing, mentioned in SO 7.1.4)	DS9.3 Configuration integrity review PC3 Process repeatability PC5 Policy, plans and procedures

Figure 13—Detailed Mapping (ITIL to CobiT) (*cont.*)	
Index of ITIL	**Linkage to CobiT**
Service Operations (*cont.*)	
SO 8 Implementing service operation	PO4.1 IT process framework
SO 9 Challenges, critical success factors and risks	DS framework level process repeatability
SO App A Complementary industry guidance	PO8.2 IT standards and quality practices
SO App B Communication in service operation	DS13.1 Operations procedures and instructions
SO App C Kepner and Tregoe	DS10.1 Identification and classification of problems
SO App D Ishikawa diagrams	DS10.1 Identification and classification of problems
SO App E Detailed description of facilities management	DS12.2 Physical security measures DS12.3 Physical access DS12.4 Protection against environmental factors
SO App F Physical access control	DS12.3 Physical access
Continuous Service Improvement	
CSI 1 Introduction	PO8.5 Continuous improvement DS1 Define and manage service levels ME1 Monitor and evaluate IT performance
CSI 2 Service management as a practice	PO8.5 Continuous improvement
CSI 3 CSI principles	PO8.5 Continuous improvement ME1.4 Performance assessment PC6 Process performance improvement
CSI 3.10 Governance	ME4.1 Establishment of an IT governance framework
CSI 3.11 Frameworks, models, standards and quality systems	PO4.1 IT process framework ME4.1 Establishment of an IT governance framework
CSI 4 Continual service improvement processes	PO4.1 IT process framework
CSI 4.1 The seven-step improvement process	PO8.5 Continuous improvement ME1.1 Monitoring approach PC6 Process performance improvement
CSI 4.1a Step 1—Define what you should measure	ME1.1 Monitoring approach
CSI 4.1b Step 2—Define what you can measure	ME1.1 Monitoring approach ME1.3 Monitoring method
CSI 4.1c Step 3—Gathering data	ME1.2 Definition and collection of monitoring data
CSI 4.1d Step 4—Processing the data	ME1.2 Definition and collection of monitoring data
CSI 4.1e Step 5—Analysing the data	ME1.4 Performance assessment
CSI 4.1f Step 6—Presenting and using the information	ME1.3 Monitoring method ME1.5 Board and executive reporting
CSI 4.1g Step 7—Implementing corrective action	ME1.6 Remedial actions
CSI 4.1.1 Integration with the rest of the lifecycle stages and service management processes	PO4.1 IT process framework PO8.5 Continuous improvement ME1.1 Monitoring approach
CSI 4.1.2 Metrics and measurement	ME1.1 Monitoring approach
CSI 4.2 Service reporting	DS1.5 Monitoring and reporting of service level achievements ME1.5 Board and executive reporting
CSI 4.3 Service measurement	DS1.5 Monitoring and reporting of service level achievements ME1.1 Monitoring approach DS3.2 Current performance and capacity DS8.5 Reporting and trend analysis ME4.6 Performance measurement
CSI 4.4 Return on investment for CSI	PO8.5 Continuous improvement ME1.1 Monitoring approach

Figure 13—Detailed Mapping (ITIL to COBIT) (*cont.*)	
Index of ITIL	**Linkage to COBIT**
Continuous Service Improvement (*cont.*)	
CSI 4.5 Business questions for CSI	PO8.5 Continuous improvement ME1.1 Monitoring approach
CSI 4.6 Service level management	PO8.5 Continuous improvement DS1 Define and manage service levels
CSI 5 CSI methods and techniques	PO8.5 Continuous improvement PC6 Process performance improvement
CSI 5.1 Methods and techniques	PO8.5 Continuous improvement ME1.1 Monitoring approach
CSI 5.2 Assessments	PO1.3 Assessment of current capability and performance PO4.1 IT process framework PO8.6 Quality measurement, monitoring and review ME1.1 Monitoring approach
CSI 5.3 Benchmarking	PO8.6 Quality measurement, monitoring and review ME1.4 Performance assessment
CSI 5.4 Measuring and reporting frameworks	PO8.6 Quality measurement, monitoring and review ME1.3 Monitoring method
CSI 5.5 The Deming Cycle	PO4.1 IT process framework PO8.5 Continuous improvement
CSI 5.6 CSI and other service management processes	PO8.5 Continuous improvement PC6 Process performance improvement
CSI 5.6.1 Availability management	DS3.4 IT resources availability
CSI 5.6.2 Capacity management	DS3.1 Performance and capacity planning
CSI 5.6.3 IT service continuity management	PO9.3 Event identification DS4.1 IT continuity framework
CSI 5.6.4 Problem management	DS10 Manage problems
CSI 5.6.5 Change, release and deployment management	AI6 Manage changes AI7 Install and accredit solutions and changes
CSI 5.6.6 Knowledge management	AI4 Enable operation and use
CSI 5.6.7 Summary	PO8.5 Continuous improvement
CSI 6 Organising for continual service improvement	PO4.6 Establishment of roles and responsibilities PO4.7 Responsibility for IT quality assurance PO8.5 Continuous improvement PC2 Process ownership PC4 Roles and responsibilities PC6 Process performance improvement
CSI 7 Technology considerations	PC3 Process repeatability PC5 Policy, plans and procedures
CSI 8 Implementing continual service improvement	PO4.1 IT process framework PO8.5 Continuous improvement ME1.4 Performance assessment
CSI 9 Challenges, critical success factors and risks	PO8.5 Continuous improvement
CSI App A Complementary guidance	PO8.2 IT standards and quality practices ME4.1 Establishment of an IT governance framework

7. SUMMARY

Every organisation needs to tailor the use of standards and practices, such as those examined in this document, to suit its individual requirements. COBIT helps to define *what* should be done and ITIL provides the *how* for service management aspects. Typical uses for the standards and practices are:

- To support governance by:
  - Providing a management policy and control framework
  - Enabling process ownership, clear responsibility and accountability for IT activities
  - Aligning IT objectives with business objectives, setting priorities and allocating resources
  - Ensuring return on investments and optimising costs
  - Making sure that significant risks have been identified and are transparent to management, responsibility for risk management has been assigned and embedded in the organisation, and assurance that effective controls are in place has been provided to management
  - Ensuring resources have been organised efficiently and sufficient capability (technical infrastructure, process and skills) exists to execute the IT strategy
  - Making sure that critical IT activities can be monitored and measured, so problems can be identified and corrective action can be taken
- To define requirements in service and project definitions, internally and with service providers. For example:
  - Improving IT service and business process alignment and integration
  - Setting clear, business-related IT objectives and metrics
  - Defining services and projects in end-user terms
  - Creating SLAs and contracts that can be monitored by customers
  - Making sure that customer requirements have been cascaded properly into technical IT operational requirements
  - Considering services and project portfolios collectively so relative priorities can be set and resources can be allocated on an equitable and achievable basis
- To verify provider capability or demonstrate competence to the market by:
  - Independent third-party assessments and audits
  - Contractual commitments
  - Attestations and certifications
- To facilitate continuous improvement by:
  - Maturity assessments
  - Gap analyses
  - Benchmarking
  - Improvement planning
  - Avoidance of reinventing already-proven good approaches
- As a framework for audit/assessment and an external view through:
  - Objective and mutually understood criteria
  - Benchmarking to justify weaknesses and gaps in control
  - Increasing the depth and value of recommendations by following generally accepted preferred approaches

IT best practices need to be aligned with business requirements and integrated with one another and with internal procedures. COBIT can be used at the highest level, providing an overall control framework based on an IT process model that should generically suit every organisation. Specific practices and standards such as ITIL cover discrete areas and can be mapped to the COBIT framework, thus providing a hierarchy of guidance materials.

8. REFERENCES

IT Governance Institute, COBIT 4.1, USA, 2007
Office of Government Commerce, *Continual Service Improvement*, UK, 2007
Office of Government Commerce, *Official Introduction to the IT Service Lifecycle*, UK, 2007
Office of Government Commerce, *Service Design*, UK, 2007
Office of Government Commerce, *Service Operation*, UK, 2007
Office of Government Commerce, *Service Strategy*, UK, 2007
Office of Government Commerce, *Service Transition*, UK, 2007
Paulk, M.C.; et al.; 'Capability Maturity Model℠ for Software', CMU/SEI-93-TR-24, Carnegie Mellon University, Software Engineering Institute, USA, 1993

APPENDIX—COBIT AND RELATED PRODUCTS

The COBIT framework, in versions 4.1 and higher, includes all of the following:

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

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

- *Board Briefing on IT Governance, 2nd Edition*—Designed to help executives understand why IT governance is important, what its issues are and what the board's responsibility is for managing it
- COBIT Online®—Allows users to customise a version of COBIT for their own enterprise, then store and manipulate that version as desired. It offers online, real-time surveys, frequently asked questions, benchmarking and a discussion facility for sharing experiences and questions.
- *COBIT® Control Practices: Guidance to Achieve Control Objectives for Successful IT Governance, 2nd Edition*—Provides guidance on the risks to be avoided and value to be gained from implementing a control objective, and instruction on how to implement the objective. Control practices are strongly recommended for use with *IT Governance Implementation Guide: Using COBIT® and Val IT™, 2nd Edition*.
- *IT Assurance Guide: Using COBIT®*—Provides guidance on how COBIT can be used to support a variety of assurance activities and offers suggested testing steps for all the COBIT IT processes and control objectives. It replaces the information in *Audit Guidelines* for auditing and self-assessment against the control objectives in COBIT® 4.1.
- *IT Control Objectives for Sarbanes-Oxley: The Role of IT in the Design and Implementation of Internal Control Over Financial Reporting, 2nd Edition*—Provides guidance on how to assure compliance for the IT environment based on the COBIT control objectives
- *IT Governance Implementation Guide: Using COBIT® and Val IT™, 2nd Edition*—Provides a generic road map for implementing IT governance using COBIT and Val IT resources and a supporting tool kit
- *COBIT® Quickstart, 2nd Edition*—Provides a baseline of control for the smaller organisation and a possible first step for the larger enterprise
- *COBIT® Security Baseline: An Information Security Survival Kit, 2nd Edition*—Focuses on essential steps for implementing information security within the enterprise
- COBIT mappings—Currently posted at *www.isaca.org/downloads*:
  - *Aligning COBIT®, ITIL and ISO 17799 for Business Benefit*
  - *COBIT® Mapping: Mapping of CMMI® for Development V1.2 With COBIT® 4.0*
  - *COBIT® Mapping: Mapping of COSO Enterprise Risk Management With COBIT® 4.1*
  - *COBIT® Mapping: Mapping of ISO/IEC 17799:2000 With COBIT®, 2nd Edition*
  - *COBIT® Mapping: Mapping of ISO/IEC 17799:2005 With COBIT® 4.0*
  - *COBIT® Mapping: Mapping of ITIL With COBIT® 4.0*
  - *COBIT® Mapping: Mapping of ITIL v3 With COBIT® 4.1*
  - *COBIT® Mapping: Mapping of PMBOK With COBIT® 4.0*
  - *COBIT® Mapping: Mapping of PRINCE2 With COBIT® 4.0*
  - *COBIT® Mapping: Mapping of SEI's CMM for Software With COBIT® 4.0*
  - *COBIT® Mapping: Mapping of TOGAF 8.1 With COBIT® 4.0*
  - *COBIT® Mapping: Overview of International IT Guidance, 2nd Edition*
- *Information Security Governance: Guidance for Boards of Directors and Executive Management, 2nd Edition*—Presents information security in business terms and contains tools and techniques to help uncover security-related problems

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

Current Val IT-related publications are:
- *Enterprise Value: Governance of IT Investments, The Val IT Framework 2.0*, which explains how an enterprise can extract optimal value from IT-enabled investments and is based on the COBIT framework. It is organised into three processes—Value Governance, Portfolio Management and Investment Management—and key management practices which are essential management practices that positively influence the achievement of the desired result or purpose of a particular activity. They support the Val IT processes and play roughly the same role as COBIT's control objectives.
- *Enterprise Value: Governance of IT Investments, Getting Started With Value Management*—This publication provides an easy-to-follow guide on getting a value management initiative started for business and IT executives and organisational leaders.
- *Enterprise Value: Governance of IT Investments, The Business Case*, which focuses on one key element of the investment management process

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

LEADING THE IT GOVERNANCE COMMUNITY

3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 USA
Phone: +1.847.660.5700
Fax: +1.847.253.1443
E-mail: *info@itgi.org*
Web site: *www.itgi.org*

ISBN 978-1-60420-035-5