IT
GOVERNANCE
INSTITUTE®

LEADING THE IT GOVERNANCE COMMUNITY

COBIT® 4.1

Framework

Control Objectives

Management Guidelines

Maturity Models

The IT Governance Institute®

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

Disclaimer

ITGI (the "Owner") has designed and created this publication, titled COBIT® 4.1 (the "Work"), primarily as an educational resource for chief information officers (CIOs), senior management, IT management and control professionals. The Owner makes no claim that use of any of the Work will assure a successful outcome. The Work should not be considered inclusive of any proper information, procedures and tests or exclusive of other information, procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific information, procedure or test, CIOs, senior management, IT management and control professionals should apply their own professional judgement to the specific circumstances presented by the particular systems or IT environment.

Disclosure

IT Governance Institute
3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 USA
Phone: +1.847.590.7491
Fax: +1.847.253.1443
E-mail: *info@itgi.org*
Web site: *www.itgi.org*

ISBN 1-933284-72-2
COBIT® 4.1
Printed in the United States of America

ACKNOWLEDGEMENTS

IT Governance Institute wishes to recognise:

Expert Developers and Reviewers

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

ACKNOWLEDGEMENTS *CONT*.

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

ITGI Board of Trustees

IT Governance Committee

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

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

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

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

TABLE OF CONTENTS

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

Executive Overview

EXECUTIVE OVERVIEW

For many enterprises, information and the technology that supports it represent their most valuable, but often least understood, assets. Successful enterprises recognise the benefits of information technology and use it to drive their stakeholders' value. These enterprises also understand and manage the associated risks, such as increasing regulatory compliance and critical dependence of many business processes on information technology (IT).

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

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

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

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

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

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

The business orientation of COBIT consists of linking business goals to IT goals, providing metrics and maturity models to measure their achievement, and identifying the associated responsibilities of business and IT process owners.

The process focus of COBIT is illustrated by a process model that subdivides IT into four domains and 34 processes in line with the responsibility areas of plan, build, run and monitor, providing an end-to-end view of IT. Enterprise architecture concepts help identify the resources essential for process success, i.e., applications, information, infrastructure and people.

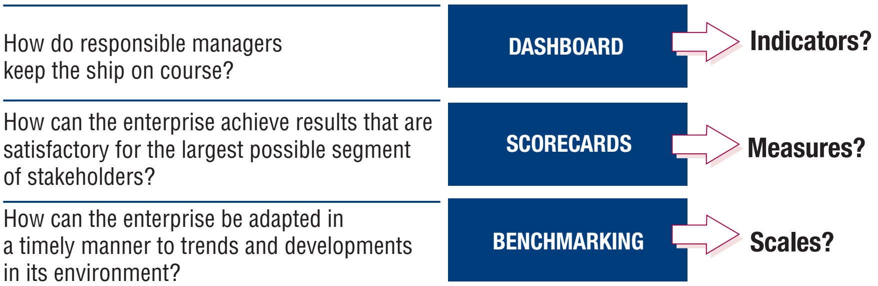
In summary, to provide the information that the enterprise needs to achieve its objectives, IT resources need to be managed by a set of naturally grouped processes.

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

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

Second, in today's complex environments, management is continuously searching for condensed and timely information to make difficult decisions on value, risk and control quickly and successfully. What should be measured, and how? Enterprises need an objective measure of where they are and where improvement is required, and they need to implement a management tool kit to monitor this improvement. **Figure 1** shows some traditional questions and the management information tools used to find the responses, but these dashboards need indicators, scorecards need measures and benchmarking needs a scale for comparison.

Figure 1—Management Information



How do responsible managers keep the ship on course? → DASHBOARD → Indicators?

How can the enterprise achieve results that are satisfactory for the largest possible segment of stakeholders? → SCORECARDS → Measures?

How can the enterprise be adapted in a timely manner to trends and developments in its environment? → BENCHMARKING → Scales?

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

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

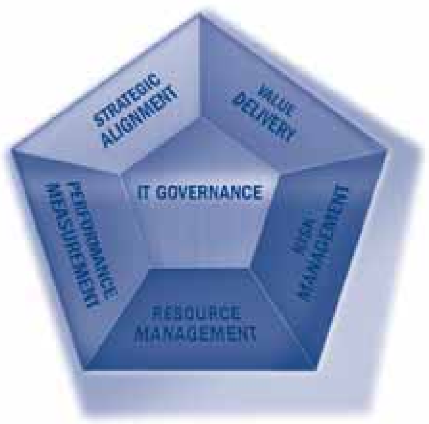
The assessment of process capability based on the COBIT maturity models is a key part of IT governance implementation. After identifying critical IT processes and controls, maturity modelling enables gaps in capability to be identified and demonstrated to management. Action plans can then be developed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

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

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

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

Figure 2—IT Governance Focus Areas



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

These IT governance focus areas describe the topics that executive management needs to address to govern IT within their enterprises. Operational management uses processes to organise and manage ongoing IT activities. COBIT provides a generic process model that represents all the processes normally found in IT functions, providing a common reference model understandable to operational IT and business managers. The COBIT process model has been mapped to the IT governance focus areas (see appendix II, Mapping IT Processes to IT Governance Focus Areas, COSO, COBIT IT Resources and COBIT Information Criteria), providing a bridge between what operational managers need to execute and what executives wish to govern.

To achieve effective governance, executives require that controls be implemented by operational managers within a defined control framework for all IT processes. COBIT's IT control objectives are organised by IT process; therefore, the framework provides a clear link among IT governance requirements, IT processes and IT controls.

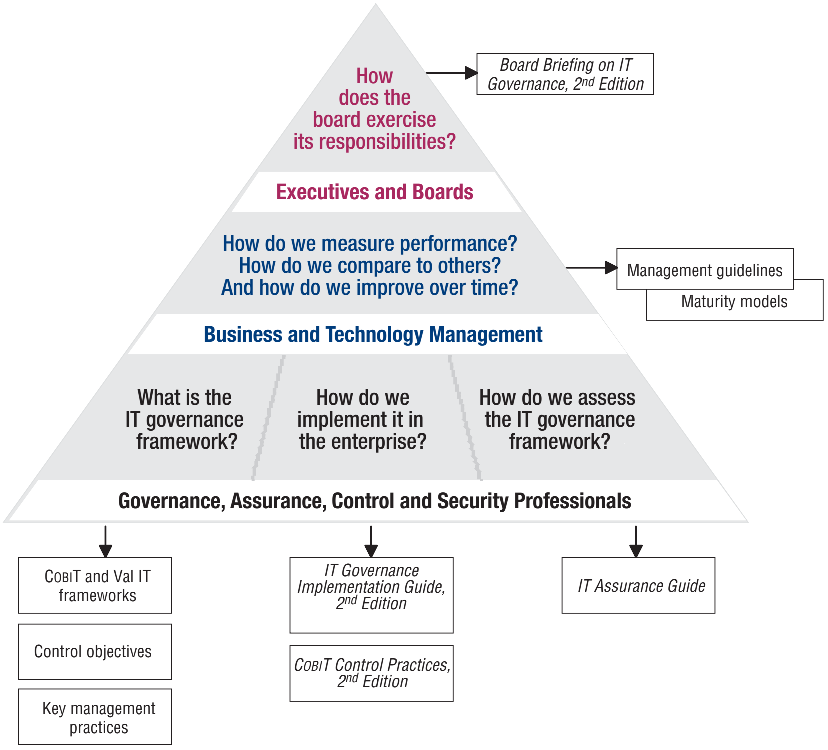
COBIT is focused on what is required to achieve adequate management and control of IT, and is positioned at a high level. COBIT has been aligned and harmonised with other, more detailed, IT standards and good practices (see appendix IV, COBIT 4.1 Primary Reference Material). COBIT acts as an integrator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

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

The COBIT products have been organised into three levels (**figure 3**) designed to support:
- Executive management and boards
- Business and IT management
- Governance, assurance, control and security professionals

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

Figure 3—COBIT Content Diagram

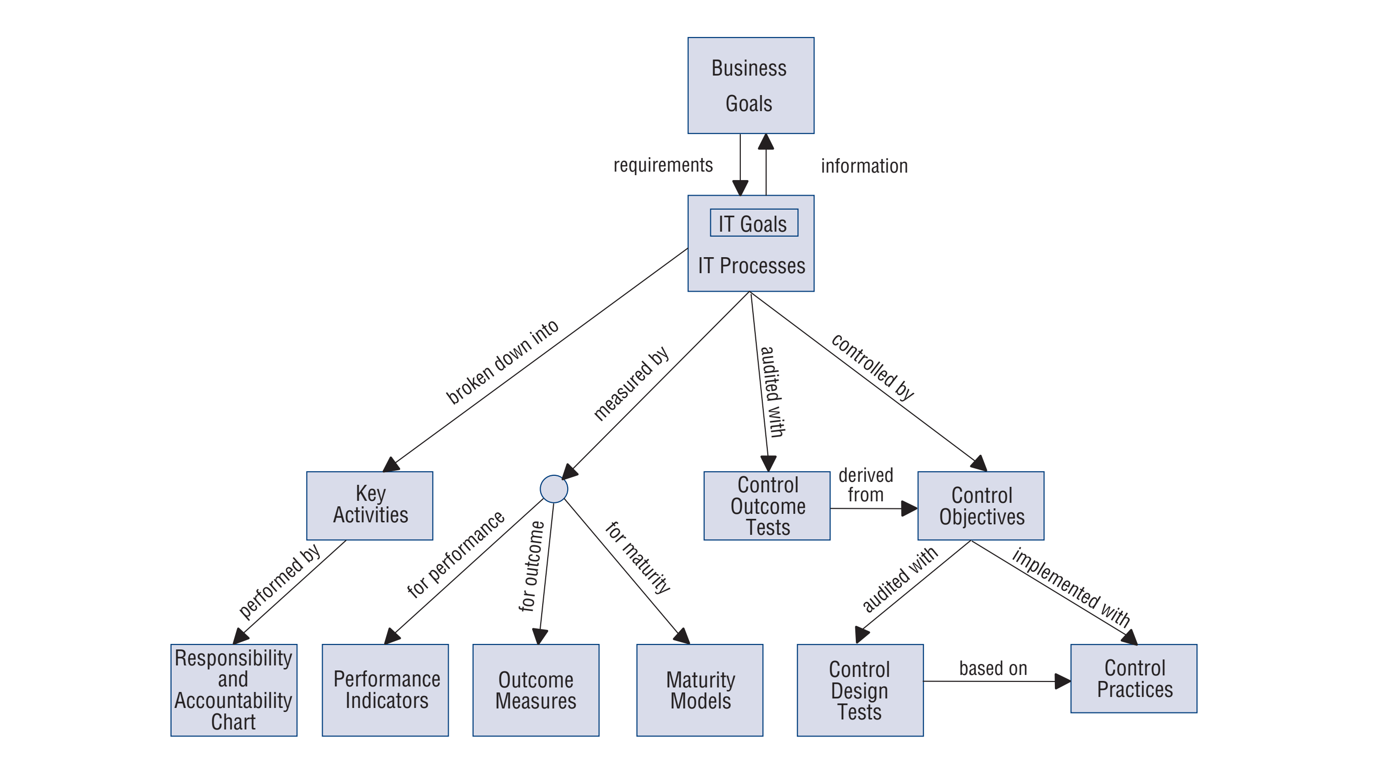

How does the board exercise its responsibilities?
Board Briefing on IT Governance, 2nd Edition
Executives and Boards
How do we measure performance? How do we compare to others? And how do we improve over time?
Management guidelines
Maturity models
Business and Technology Management
What is the IT governance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

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

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

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

Figure 4—Interrelationships of COBIT Components



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

The benefits of implementing COBIT as a governance framework over IT include:
- Better alignment, based on a business focus
- A view, understandable to management, of what IT does
- Clear ownership and responsibilities, based on process orientation
- General acceptability with third parties and regulators
- Shared understanding amongst all stakeholders, based on a common language
- Fulfilment of the COSO requirements for the IT control environment

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

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

CobiT Framework

COBIT FRAMEWORK

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

THE NEED FOR A CONTROL FRAMEWORK FOR IT GOVERNANCE

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

Why

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

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

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

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

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

Who

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

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

What

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

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

HOW COBIT MEETS THE NEED

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

Business-focused

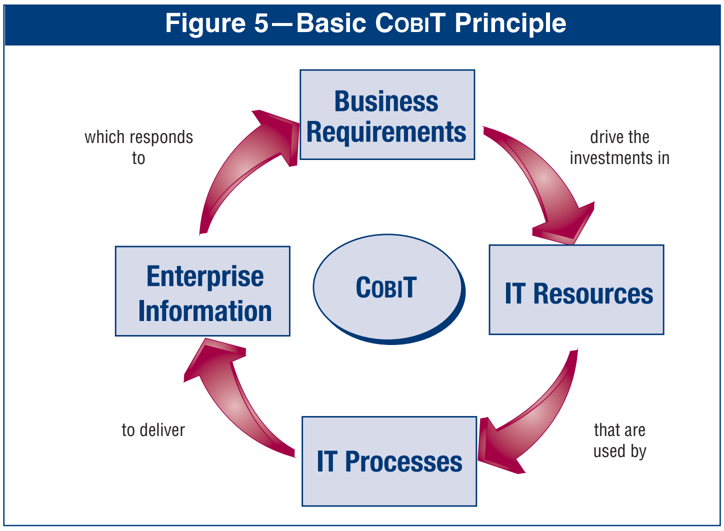
Business orientation is the main theme of COBIT. It is designed not only to be employed by IT service providers, users and auditors, but also, and more important, to provide comprehensive guidance for management and business process owners.

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

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

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

Figure 5—Basic COBIT Principle



COBIT'S INFORMATION CRITERIA

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

- **Effectiveness** deals with information being relevant and pertinent to the business process as well as being delivered in a timely, correct, consistent and usable manner.
- **Efficiency** concerns the provision of information through the optimal (most productive and economical) use of resources.
- **Confidentiality** concerns the protection of sensitive information from unauthorised disclosure.

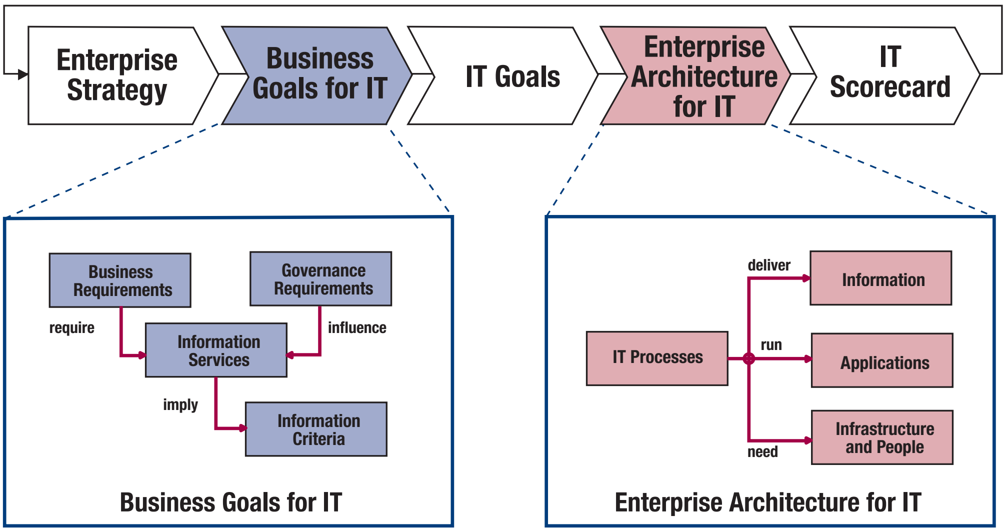
- **Integrity** relates to the accuracy and completeness of information as well as to its validity in accordance with business values and expectations.
- **Availability** relates to information being available when required by the business process now and in the future. It also concerns the safeguarding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

BUSINESS GOALS AND IT GOALS

Whilst information criteria provide a generic method for defining the business requirements, defining a set of generic business and IT goals provides a business-related and more refined basis for establishing business requirements and developing the metrics that allow measurement against these goals. Every enterprise uses IT to enable business initiatives, and these can be represented as business goals for IT. Appendix I provides a matrix of generic business goals and IT goals and shows how they map to the information criteria. These generic examples can be used as a guide to determine the specific business requirements, goals and metrics for the enterprise.

If IT is to successfully deliver services to support the enterprise's strategy, there should be a clear ownership and direction of the requirements by the business (the customer) and a clear understanding of what needs to be delivered, and how, by IT (the provider). **Figure 6** illustrates how the enterprise strategy should be translated by the business into objectives related to IT-enabled initiatives (the business goals for IT). These objectives should lead to a clear definition of IT's own objectives (the IT goals), which in turn define the IT resources and capabilities (the enterprise architecture for IT) required to successfully execute IT's part of the enterprise's strategy.[1]

Figure 6—Defining IT Goals and Enterprise Architecture for IT



Once the aligned goals have been defined, they need to be monitored to ensure that actual delivery matches expectations. This is achieved by metrics that are derived from the goals and captured in an IT scorecard.

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

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

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

IT RESOURCES

The IT organisation delivers against these goals by a clearly defined set of processes that use people skills and technology infrastructure to run automated business applications while leveraging business information. These resources, together with the processes, constitute an enterprise architecture for IT, as shown in **figure 6**.

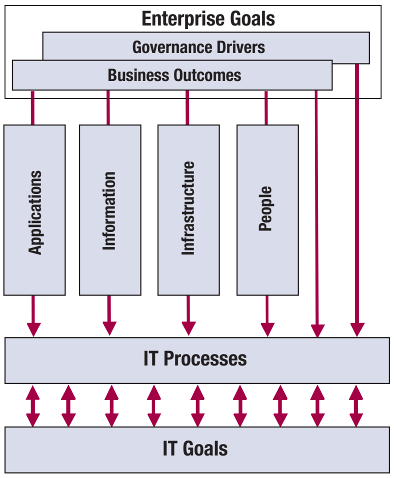
To respond to the business requirements for IT, the enterprise needs to invest in the resources required to create an adequate technical capability (e.g., an enterprise resource planning [ERP] system) to support a business capability (e.g., implementing a supply chain) resulting in the desired outcome (e.g., increased sales and financial benefits).

The IT resources identified in COBIT can be defined as follows:

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

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

Figure 7—Managing IT Resources to Deliver IT Goals



Process-oriented

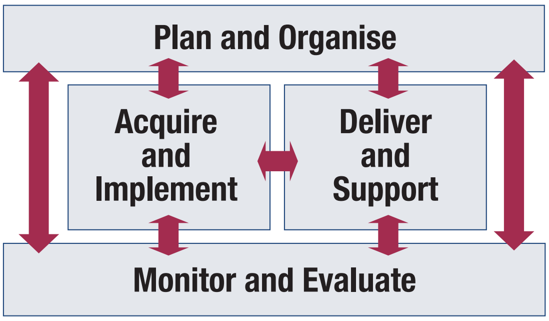
COBIT defines IT activities in a generic process model within four domains. These domains are Plan and Organise, Acquire and Implement, Deliver and Support, and Monitor and Evaluate. The domains map to IT's traditional responsibility areas of plan, build, run and monitor.

The COBIT framework provides a reference process model and common language for everyone in an enterprise to view and manage IT activities. Incorporating an operational model and a common language for all parts of the business involved in IT is one of the most important and initial steps toward good governance. It also provides a framework for measuring and monitoring IT performance, communicating with service providers and integrating best management practices. A process model encourages process ownership, enabling responsibilities and accountability to be defined.

To govern IT effectively, it is important to appreciate the activities and risks within IT that need to be managed. They are usually ordered into the responsibility domains of plan, build, run and monitor. Within the COBIT framework, these domains, as shown in **figure 8**, are called:

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

Figure 8—The Four Interrelated Domains of COBIT



PLAN AND ORGANISE (PO)

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

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

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

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

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

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

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

- Is IT's performance measured to detect problems before it is too late?
- Does management ensure that internal controls are effective and efficient?
- Can IT performance be linked back to business goals?
- Are adequate confidentiality, integrity and availability controls in place for information security?

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

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

Controls-based

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

PROCESSES NEED CONTROLS
Control is defined as the policies, procedures, practices and organisational structures designed to provide reasonable assurance that business objectives will be achieved and undesired events will be prevented or detected and corrected.

IT control objectives provide a complete set of high-level requirements to be considered by management for effective control of each IT process. They:

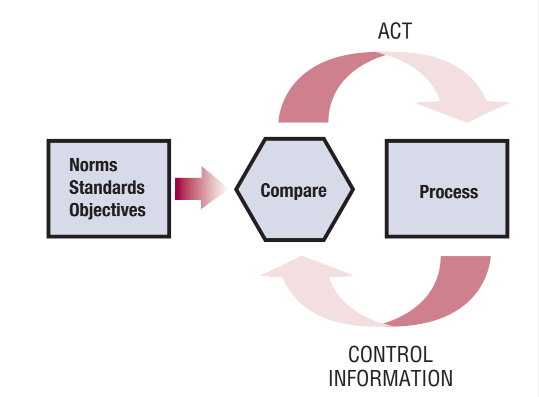
- Are statements of managerial actions to increase value or reduce risk
- Consist of policies, procedures, practices and organisational structures
- Are designed to provide reasonable assurance that business objectives will be achieved and undesired events will be prevented or detected and corrected

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

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

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

Figure 9—Control Model



Operational management uses processes to organise and manage ongoing IT activities. COBIT provides a generic process model that represents all the processes normally found in IT functions, providing a common reference model understandable to operational IT and business managers. To achieve effective governance, controls need to be implemented by operational managers within a defined control framework for all IT processes. Since COBIT's IT control objectives are organised by IT process, the framework provides clear links amongst IT governance requirements, IT processes and IT controls.

Each of COBIT's IT processes has a process description and a number of control objectives. As a whole, they are the characteristics of a well-managed process.

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

PC1 Process Goals and Objectives
Define and communicate specific, measurable, actionable, realistic, results-oriented and timely (SMARRT) process goals and objectives for the effective execution of each IT process. Ensure that they are linked to the business goals and supported by suitable metrics.

PC2 Process Ownership
Assign an owner for each IT process, and clearly define the roles and responsibilities of the process owner. Include, for example, responsibility for process design, interaction with other processes, accountability for the end results, measurement of process performance and the identification of improvement opportunities.

PC3 Process Repeatability
Design and establish each key IT process such that it is repeatable and consistently produces the expected results. Provide for a logical but flexible and scaleable sequence of activities that will lead to the desired results and is agile enough to deal with exceptions and emergencies. Use consistent processes, where possible, and tailor only when unavoidable.

PC4 Roles and Responsibilities
Define the key activities and end deliverables of the process. Assign and communicate unambiguous roles and responsibilities for effective and efficient execution of the key activities and their documentation as well as accountability for the process end deliverables.

PC5 Policy, Plans and Procedures
Define and communicate how all policies, plans and procedures that drive an IT process are documented, reviewed, maintained, approved, stored, communicated and used for training. Assign responsibilities for each of these activities and, at appropriate times, review whether they are executed correctly. Ensure that the policies, plans and procedures are accessible, correct, understood and up to date.

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

Effective controls reduce risk, increase the likelihood of value delivery and improve efficiency because there will be fewer errors and a more consistent management approach.

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

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

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

BUSINESS AND IT CONTROLS

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

- At the executive management level, business objectives are set, policies are established and decisions are made on how to deploy and manage the resources of the enterprise to execute the enterprise strategy. The overall approach to governance and control is established by the board and communicated throughout the enterprise. The IT control environment is directed by this top-level set of objectives and policies.
- At the business process level, controls are applied to specific business activities. Most business processes are automated and integrated with IT application systems, resulting in many of the controls at this level being automated as well. These controls are known as application controls. However, some controls within the business process remain as manual procedures, such as authorisation for transactions, separation of duties and manual reconciliations. Therefore, controls at the business process level are a combination of manual controls operated by the business and automated business and application controls. Both are the responsibility of the business to define and manage, although the application controls require the IT function to support their design and development.
- To support the business processes, IT provides IT services, usually in a shared service to many business processes, as many of the development and operational IT processes are provided to the whole enterprise, and much of the IT infrastructure is provided as a common service (e.g., networks, databases, operating systems and storage). The controls applied to all IT service activities are known as IT general controls. The reliable operation of these general controls is necessary for reliance to be placed on application controls. For example, poor change management could jeopardise (accidentally or deliberately) the reliability of automated integrity checks.

IT GENERAL CONTROLS AND APPLICATION CONTROLS

General controls are controls embedded in IT processes and services. Examples include:

- Systems development
- Change management
- Security
- Computer operations

Controls embedded in business process applications are commonly referred to as application controls. Examples include:

- Completeness
- Accuracy
- Validity
- Authorisation
- Segregation of duties

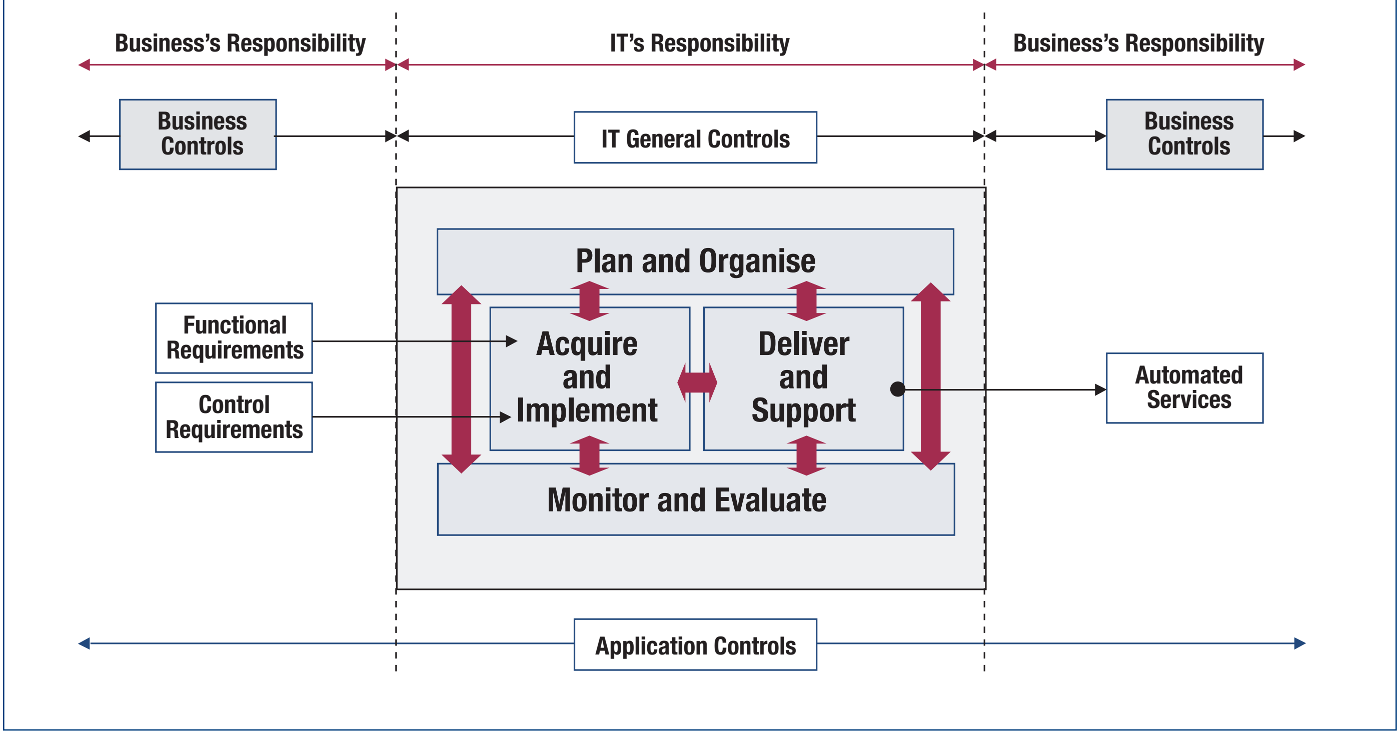
COBIT assumes the design and implementation of automated application controls to be the responsibility of IT, covered in the Acquire and Implement domain, based on business requirements defined using COBIT's information criteria, as shown in **figure 10**. The operational management and control responsibility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

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

- The business is responsible to properly:
  - Define functional and control requirements
  - Use automated services
- IT is responsible to:
  - Automate and implement business functional and control requirements
  - Establish controls to maintain the integrity of applications controls

Therefore, the COBIT IT processes cover general IT controls, but only the development aspects of application controls; responsibility for definition and operational usage is with the business.

Figure 10—Boundaries of Business, General and Application Controls



The following list provides a recommended set of application control objectives. They are identified by ACn, for application control number.

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

AC2 Source Data Collection and Entry
Establish that data input is performed in a timely manner by authorised and qualified staff. Correction and resubmission of data that were erroneously input should be performed without compromising original transaction authorisation levels. Where appropriate for reconstruction, retain original source documents for the appropriate amount of time.

AC3 Accuracy, Completeness and Authenticity Checks
Ensure that transactions are accurate, complete and valid. Validate data that were input, and edit or send back for correction as close to the point of origination as possible.

AC4 Processing Integrity and Validity
Maintain the integrity and validity of data throughout the processing cycle. Detection of erroneous transactions does not disrupt the processing of valid transactions.

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

AC6 Transaction Authentication and Integrity
Before passing transaction data between internal applications and business/operational functions (in or outside the enterprise), check it for proper addressing, authenticity of origin and integrity of content. Maintain authenticity and integrity during transmission or transport.

Measurement-driven

A basic need for every enterprise is to understand the status of its own IT systems and to decide what level of management and control the enterprise should provide. To decide on the right level, management should ask itself: How far should we go, and is the cost justified by the benefit?

Obtaining an objective view of an enterprise's own performance level is not easy. What should be measured and how? Enterprises need to measure where they are and where improvement is required, and implement a management tool kit to monitor this improvement. COBIT deals with these issues by providing:
- Maturity models to enable benchmarking and identification of necessary capability improvements
- Performance goals and metrics for the IT processes, demonstrating how processes meet business and IT goals and are used for measuring internal process performance based on balanced scorecard principles
- Activity goals for enabling effective process performance

MATURITY MODELS

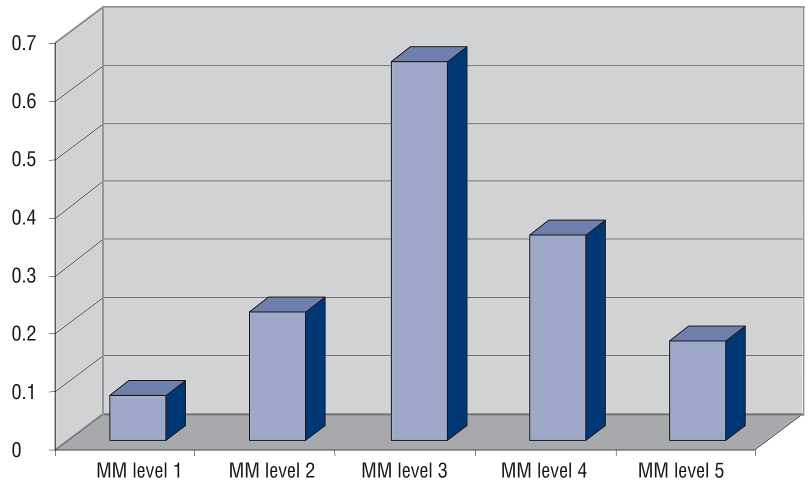
Senior managers in corporate and public enterprises are increasingly asked to consider how well IT is being managed. In response to this, business cases require development for improvement and reaching the appropriate level of management and control over the information infrastructure. While few would argue that this is not a good thing, they need to consider the cost-benefit balance and these related questions:
- What are our industry peers doing, and how are we placed in relation to them?
- What is acceptable industry good practice, and how are we placed with regard to these practices?
- Based upon these comparisons, can we be said to be doing enough?
- How do we identify what is required to be done to reach an adequate level of management and control over our IT processes?

It can be difficult to supply meaningful answers to these questions. IT management is constantly on the lookout for benchmarking and self-assessment tools in response to the need to know what to do in an efficient manner. Starting from COBIT's processes, the process owner should be able to incrementally benchmark against that control objective. This responds to three needs:
1. A relative measure of where the enterprise is
2. A manner to efficiently decide where to go
3. A tool for measuring progress against the goal

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

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

Figure 11—Possible Maturity Level of an IT Process



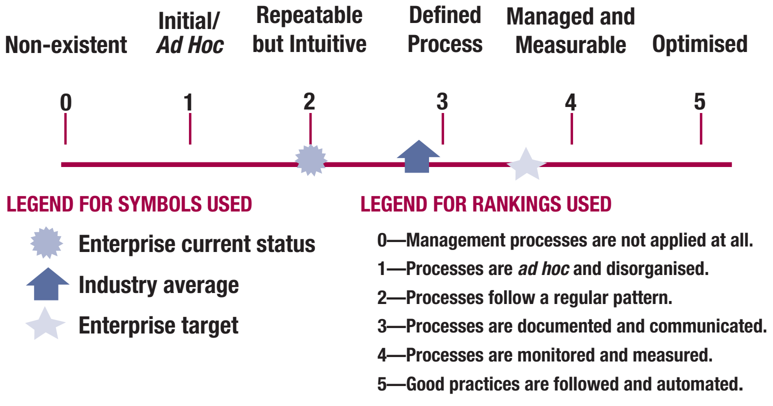
Possible maturity level of an IT process: The example illustrates a process that is largely at level 3 but still has some compliance issues with lower level requirements whilst already investing in performance measurement (level 4) and optimisation (level 5)

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

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

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

Figure 12—Graphic Representation of Maturity Models



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

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

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

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

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

Figure 13—Generic Maturity Model

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

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

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

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

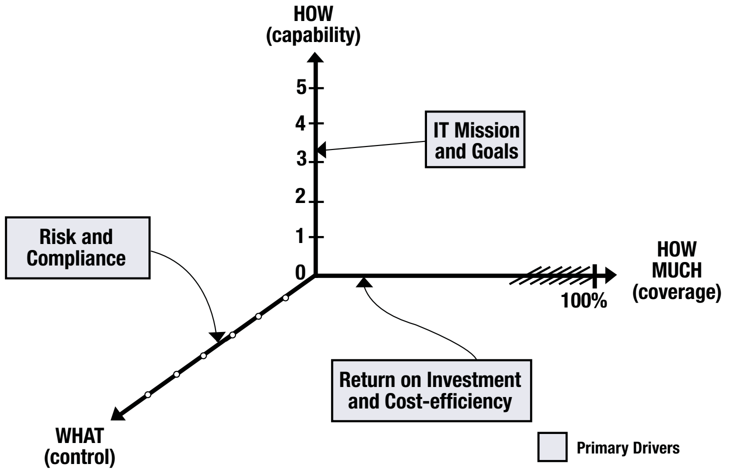
4 Managed and Measurable—Management monitors and measures compliance with procedures and takes action where processes appear not to be working effectively. Processes are under constant improvement and provide good practice. Automation and tools are used in a limited or fragmented way.

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

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

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

Figure 14—The Three Dimensions of Maturity



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

The maturity model scales will help professionals explain to managers where IT process management shortcomings exist and set targets for where they need to be. The right maturity level will be influenced by the enterprise's business objectives, the operating environment and industry practices. Specifically, the level of management maturity will depend on the enterprise's dependence on IT, its technology sophistication and, most important, the value of its information.

A strategic reference point for an enterprise to improve management and control of IT processes can be found by looking at emerging international standards and best-in-class practices. The emerging practices of today may become the expected level of performance of tomorrow and, therefore, are useful for planning where an enterprise wants to be over time.

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

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

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

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

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

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

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

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

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

PERFORMANCE MEASUREMENT

Goals and metrics are defined in COBIT at three levels:

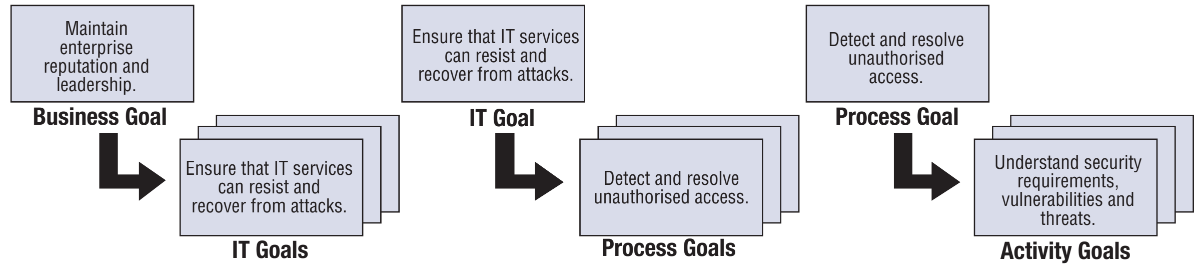
- IT goals and metrics that define what the business expects from IT and how to measure it
- Process goals and metrics that define what the IT process must deliver to support IT's objectives and how to measure it
- Activity goals and metrics that establish what needs to happen inside the process to achieve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

Figure 15—Maturity Attribute Table

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

Goals are defined top-down in that a business goal will determine a number of IT goals to support it. An IT goal is achieved by one process or the interaction of a number of processes. Therefore, IT goals help define the different process goals. In turn, each process goal requires a number of activities, thereby establishing the activity goals. **Figure 16** provides examples of the business, IT, process and activity goal relationship.

Figure 16—Example of Goal Relationships

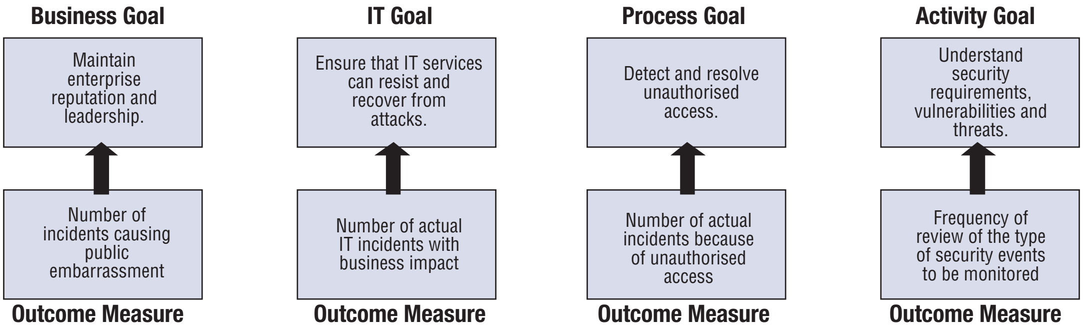

Maintain enterprise reputation and leadership.
Business Goal
Ensure that IT services can resist and recover from attacks.
IT Goals
Ensure that IT services can resist and recover from attacks.
IT Goal
Detect and resolve unauthorised access.
Process Goals
Detect and resolve unauthorised access.
Process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

The terms KGI and KPI, used in previous versions of COBIT, have been replaced with two types of metrics:

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

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

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


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

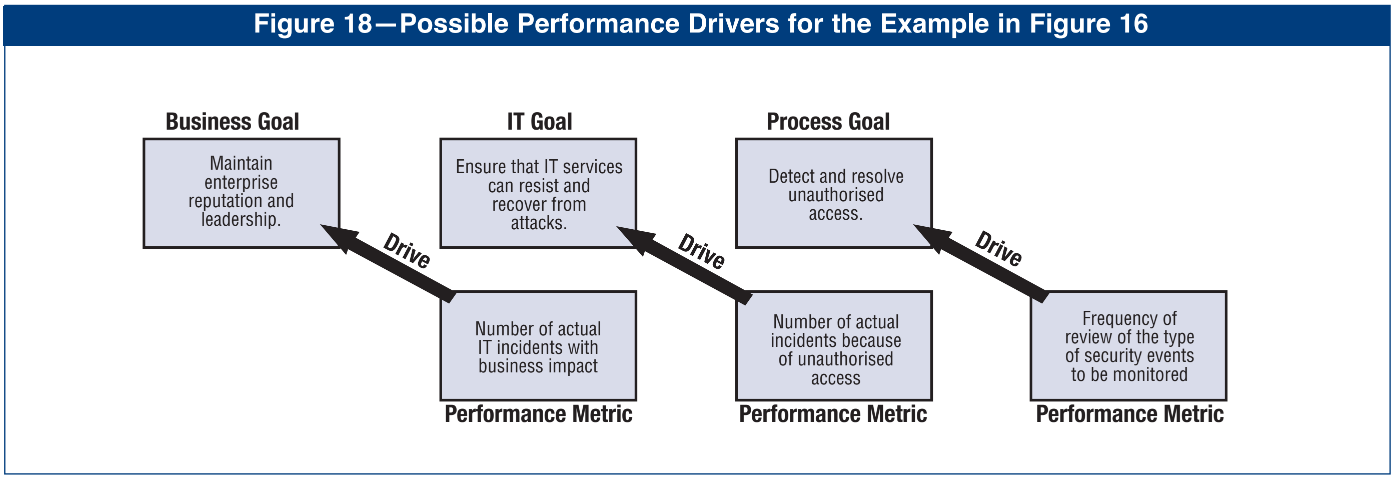
The outome measures of the lower level become performance indicators for the higher level. As per the example in **figure 16**, an outcome measure indicating that detection and resolution of unauthorised access are on target will also indicate that it will be more likely that IT services can resist and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

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

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

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

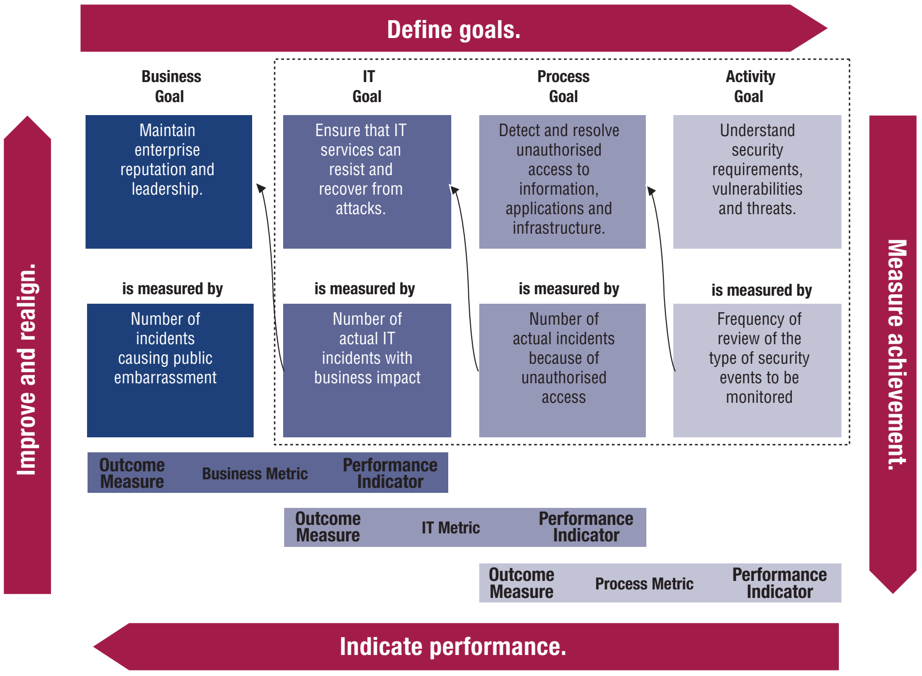
Figure 18—Possible Performance Drivers for the Example in Figure 16


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

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

Figure 19 illustrates the relationship between the business, IT, process and activity goals, and the different metrics. From top left to top right, the goals cascade is illustrated. Below the goal is the outcome measure for the goal. The small arrow indicates that the same metric is a performance indicator for the higher-level goal.

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

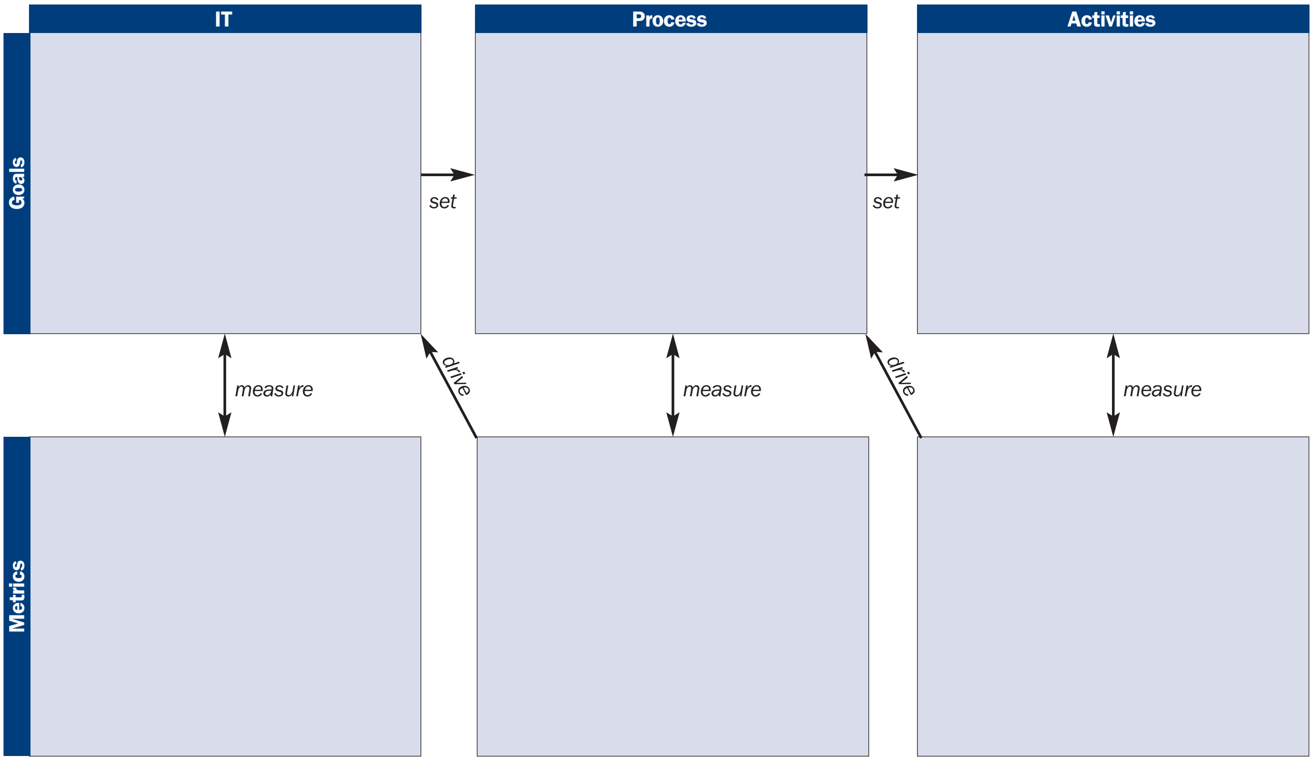

Define goals.
Business Goal
IT Goal
Process Goal
Activity Goal
Maintain enterprise reputation and leadership.
Ensure that IT services can resist and recover from attacks.
Detect and resolve unauthorised access to information, applications and infrastructure.
Understand security requirements, vulnerabilities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

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

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

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

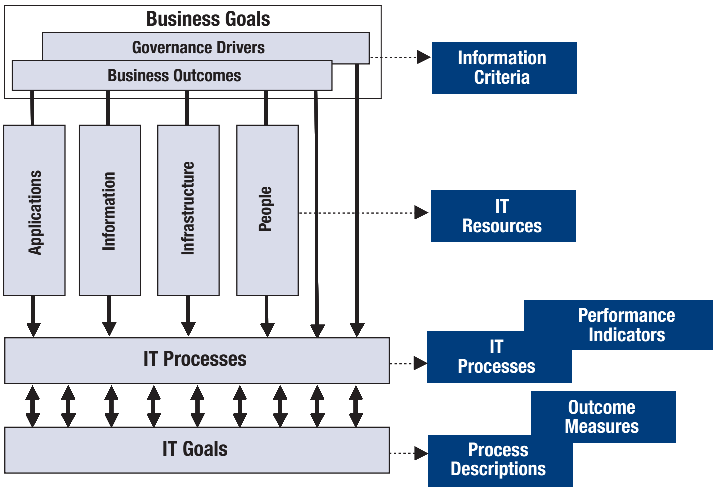
Figure 20—Presentation of Goals and Metrics



The COBIT Framework Model

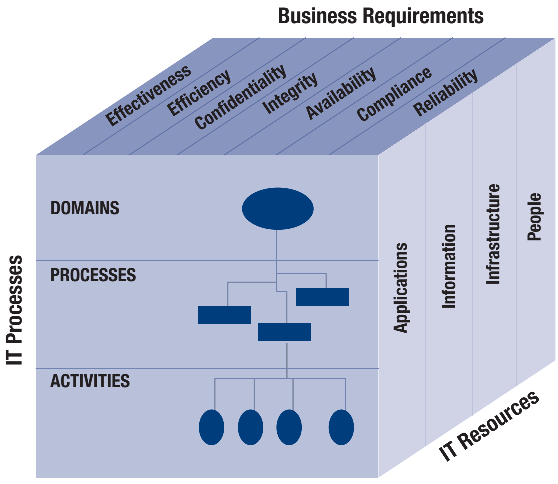
The COBIT framework, therefore, ties the businesses requirements for information and governance to the objectives of the IT services function. The COBIT process model enables IT activities and the resources that support them to be properly managed and controlled based on COBIT's control objectives, and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

Figure 21—COBIT Management, Control, Alignment and Monitoring



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

Figure 22—The COBIT Cube



In more detail, the overall COBIT framework can be shown graphically, as depicted in **figure 23**, with COBIT's process model of four domains containing 34 generic processes, managing the IT resources to deliver information to the business according to business and governance requirements.

COBIT's General Acceptability

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

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

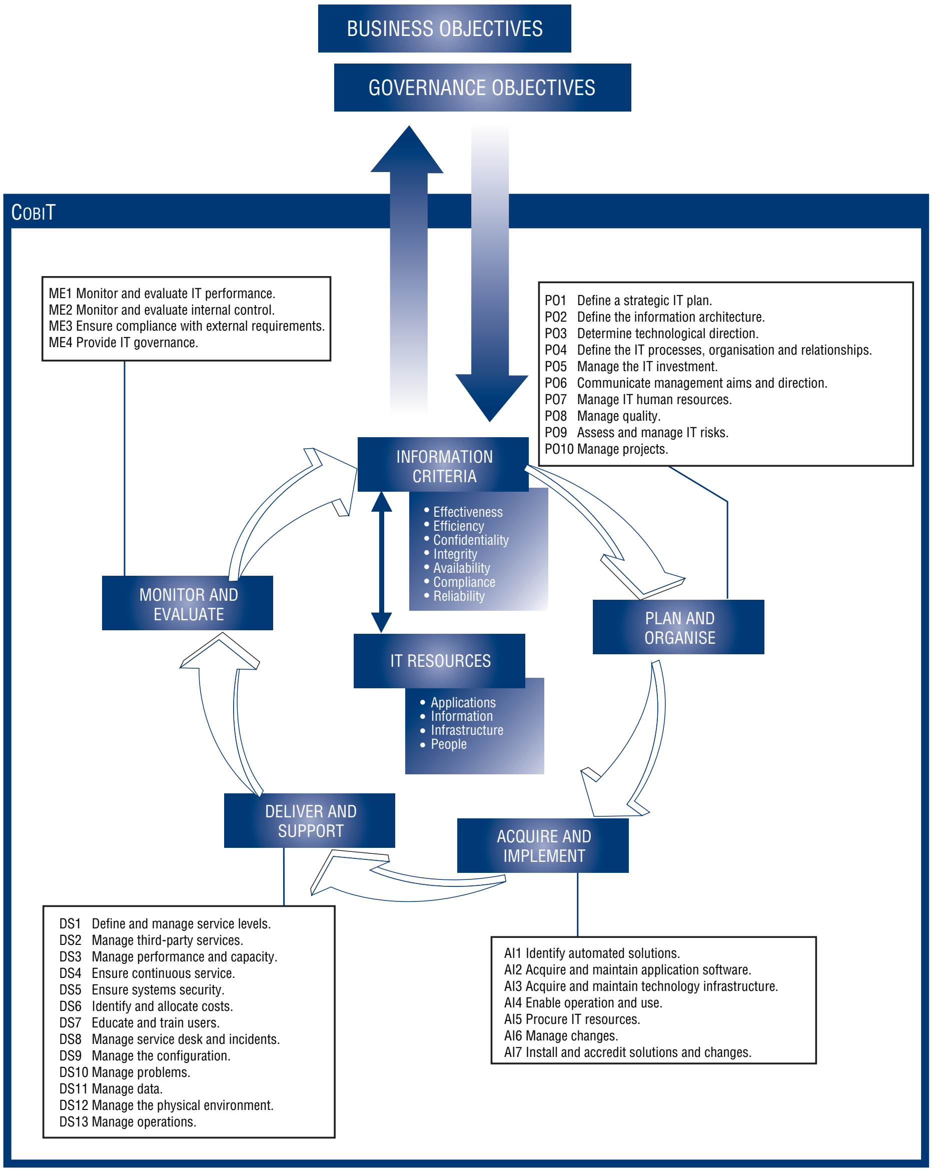
To achieve alignment of good practice to business requirements, it is recommended that COBIT be used at the highest level, providing an overall control framework based on an IT process model that should generically suit every enterprise. Specific practices and standards covering discrete areas can be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

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

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

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

Figure 23—Overall COBIT Framework



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

PO1 Define a strategic IT plan.
PO2 Define the information architecture.
PO3 Determine technological direction.
PO4 Define the IT processes, organisation and relationships.
PO5 Manage the IT investment.
PO6 Communicate management aims and direction.
PO7 Manage IT human resources.
PO8 Manage quality.
PO9 Assess and manage IT risks.
PO10 Manage projects.

DS1 Define and manage service levels.
DS2 Manage third-party services.
DS3 Manage performance and capacity.
DS4 Ensure continuous service.
DS5 Ensure systems security.
DS6 Identify and allocate costs.
DS7 Educate and train users.
DS8 Manage service desk and incidents.
DS9 Manage the configuration.
DS10 Manage problems.
DS11 Manage data.
DS12 Manage the physical environment.
DS13 Manage operations.

AI1 Identify automated solutions.
AI2 Acquire and maintain application software.
AI3 Acquire and maintain technology infrastructure.
AI4 Enable operation and use.
AI5 Procure IT resources.
AI6 Manage changes.
AI7 Install and accredit solutions and changes.

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

Figure 24—COBIT Framework and IT Governance Focus Areas

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

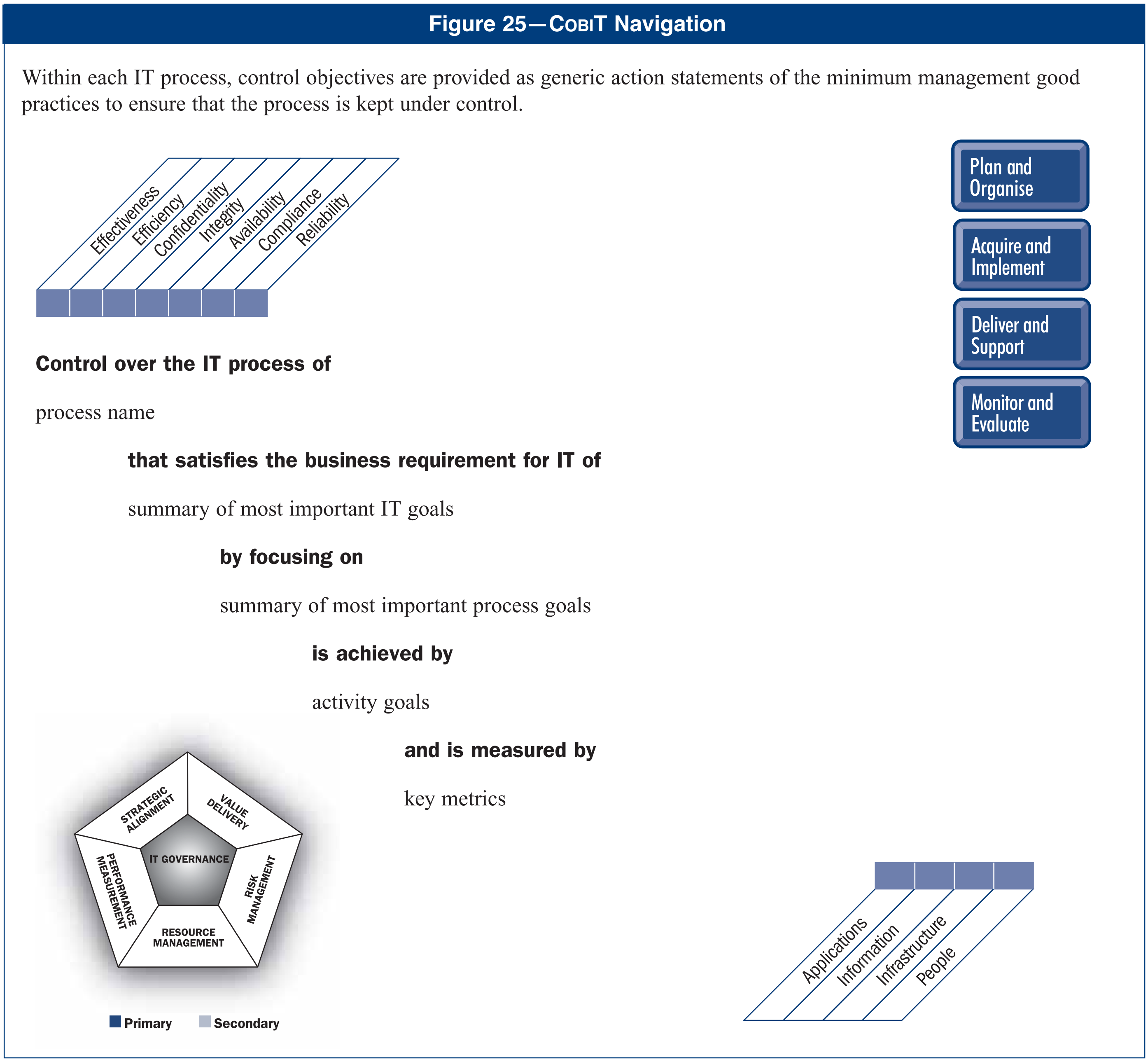
P=Primary enabler S=Secondary enabler

HOW TO USE THIS BOOK

COBIT Framework Navigation

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

Figure 25—COBIT Navigation



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

Control over the IT process of

process name

that satisfies the business requirement for IT of

summary of most important IT goals

by focusing on

summary of most important process goals

is achieved by

activity goals

and is measured by

key metrics

Overview of Core COBIT Components

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

- Section 1 (**figure 25**) contains a process description summarising the process objectives, with the process description represented in a waterfall. This page also shows the mapping of the process to the information criteria, IT resources and IT governance focus areas by way of P to indicate primary relationship and S to indicate secondary.
- Section 2 contains the control objectives for this process.
- Section 3 contains the process inputs and outputs, RACI chart, goals and metrics.
- Section 4 contains the maturity model for the process.

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

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

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

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

Users of the COBIT Components

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

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

All potential users can benefit from using the COBIT content as an overall approach to managing and governing IT, together with more detailed standards such as:
- ITIL for service delivery
- CMM for solution delivery
- ISO 17799 for information security
- PMBOK or PRINCE2 for project management

Appendices

The following additional reference sections are provided at the end of the book:

I. Tables Linking Goals and Processes (three tables)
II. Mapping IT Processes to IT Governance Focus Areas, COSO, COBIT IT Resources and COBIT Information Criteria
III. Maturity Model for Internal Control
IV. COBIT 4.1 Primary Reference Material
V. Cross-references Between COBIT® 3rd Edition© and COBIT 4.1
VI. Approach to Research and Development
VII. Glossary
VIII. COBIT and Related Products

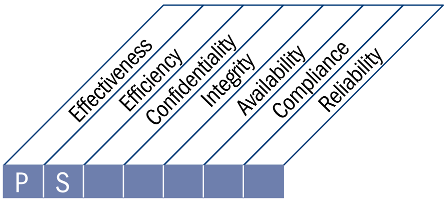
PLAN AND ORGANISE

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

Process Description

PO1 Define a Strategic IT Plan

IT strategic planning is required to manage and direct all IT resources in line with the business strategy and priorities. The IT function and business stakeholders are responsible for ensuring that optimal value is realised from project and service portfolios. The strategic plan improves key stakeholders' understanding of IT opportunities and limitations, assesses current performance, identifies capacity and human resource requirements, and clarifies the level of investment required. The business strategy and priorities are to be reflected in portfolios and executed by the IT tactical plan(s), which specifies concise objectives, action plans and tasks that are understood and accepted by both business and IT.



Plan and Organise
Acquire and Implement
Deliver and Support
Monitor and Evaluate

Control over the IT process of

Define a strategic IT plan

that satisfies the business requirement for IT of

sustaining or extending the business strategy and governance requirements whilst being transparent about benefits, costs and risks

by focusing on

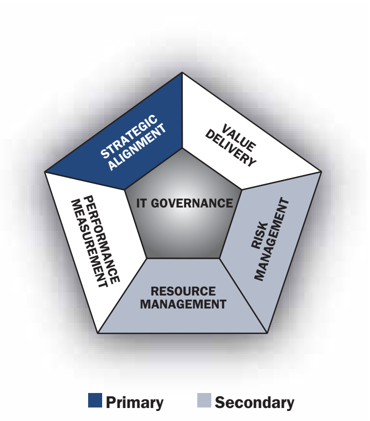
incorporating IT and business management in the translation of business requirements into service offerings, and the development of strategies to deliver these services in a transparent and effective manner

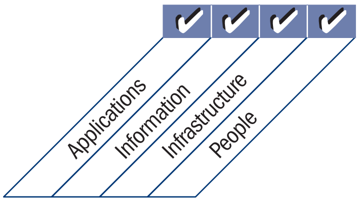
is achieved by

- Engaging with business and senior management in aligning IT strategic planning with current and future business needs
- Understanding current IT capabilities
- Providing for a prioritisation scheme for the business objectives that quantifies the business requirements

and is measured by

- Percent of IT objectives in the IT strategic plan that support the strategic business plan
- Percent of IT projects in the IT project portfolio that can be directly traced back to the IT tactical plans
- Delay between updates of IT strategic plan and updates of IT tactical plans





Control Objectives

PO1 Define a Strategic IT Plan

PO1.1 IT Value Management
Work with the business to ensure that the enterprise portfolio of IT-enabled investments contains programmes that have solid business cases. Recognise that there are mandatory, sustaining and discretionary investments that differ in complexity and degree of freedom in allocating funds. IT processes should provide effective and efficient delivery of the IT components of programmes and early warning of any deviations from plan, including cost, schedule or functionality, that might impact the expected outcomes of the programmes. IT services should be executed against equitable and enforceable service level agreements (SLAs). Accountability for achieving the benefits and controlling the costs should be clearly assigned and monitored. Establish fair, transparent, repeatable and comparable evaluation of business cases, including financial worth, the risk of not delivering a capability and the risk of not realising the expected benefits.

PO1.2 Business-IT Alignment
Establish processes of bi-directional education and reciprocal involvement in strategic planning to achieve business and IT alignment and integration. Mediate between business and IT imperatives so priorities can be mutually agreed.

PO1.3 Assessment of Current Capability and Performance
Assess the current capability and performance of solution and service delivery to establish a baseline against which future requirements can be compared. Define performance in terms of IT's contribution to business objectives, functionality, stability, complexity, costs, strengths and weaknesses.

PO1.4 IT Strategic Plan
Create a strategic plan that defines, in co-operation with relevant stakeholders, how IT goals will contribute to the enterprise's strategic objectives and related costs and risks. It should include how IT will support IT-enabled investment programmes, IT services and IT assets. IT should define how the objectives will be met, the measurements to be used and the procedures to obtain formal sign-off from the stakeholders. The IT strategic plan should cover investment/operational budget, funding sources, sourcing strategy, acquisition strategy, and legal and regulatory requirements. The strategic plan should be sufficiently detailed to allow for the definition of tactical IT plans.

PO1.5 IT Tactical Plans
Create a portfolio of tactical IT plans that are derived from the IT strategic plan. The tactical plans should address IT-enabled programme investments, IT services and IT assets. The tactical plans should describe required IT initiatives, resource requirements, and how the use of resources and achievement of benefits will be monitored and managed. The tactical plans should be sufficiently detailed to allow the definition of project plans. Actively manage the set of tactical IT plans and initiatives through analysis of project and service portfolios.

PO1.6 IT Portfolio Management
Actively manage with the business the portfolio of IT-enabled investment programmes required to achieve specific strategic business objectives by identifying, defining, evaluating, prioritising, selecting, initiating, managing and controlling programmes. This should include clarifying desired business outcomes, ensuring that programme objectives support achievement of the outcomes, understanding the full scope of effort required to achieve the outcomes, assigning clear accountability with supporting measures, defining projects within the programme, allocating resources and funding, delegating authority, and commissioning required projects at programme launch.

Management Guidelines

PO1 Define a Strategic IT Plan

From	Inputs
PO5	Cost-benefits reports
PO9	Risk assessment
PO10	Updated IT project portfolio
DS1	New/updated service requirements; updated IT service portfolio
*	Business strategy and priorities
*	Programme portfolio
ME1	Performance input to IT planning
ME4	Report on IT governance status; enterprise strategic direction for IT

* Inputs from outside CobiT

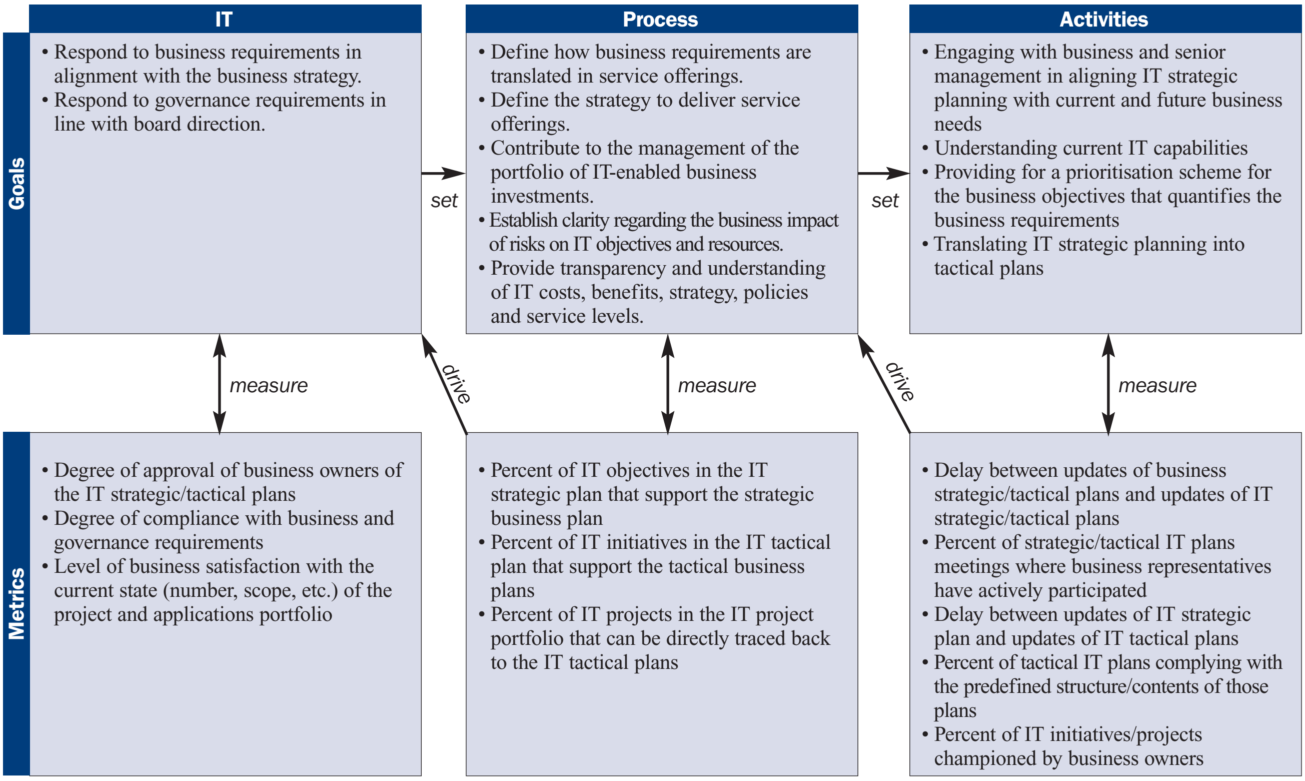
Outputs	To						
Strategic IT plan	PO2…PO6	PO8	PO9	AI1	DS1		
Tactical IT plans	PO2…PO6	PO9	AI1	DS1			
IT project portfolio	PO5	PO6	PO10	AI6			
IT service portfolio	PO5	PO6	PO9	DS1			
IT sourcing strategy	DS2						
IT acquisition strategy	AI5						

RACI Chart

Activities / Functions	CEO	CFO	Business Executive	CIO	Business Process Owner	Head Operations	Chief Architect	Head Development	Head IT Administration	PMO	Compliance, Audit, Risk and Security
Link business goals to IT goals.	C	I	A/R	R	C						
Identify critical dependencies and current performance.	C	C	R	A/R	C	C	C	C	C		C
Build an IT strategic plan.	A	C	C	R	I	C	C	C	C	I	C
Build IT tactical plans.	C	I		A	C	C	C	C	C	R	I
Analyse programme portfolios and manage project and service portfolios.	C	I	I	A	R	R	C	R	C	C	I

A **RACI** chart identifies who is **R**esponsible, **A**ccountable, **C**onsulted and/or **I**nformed.

Goals and Metrics



IT

- Respond to business requirements in alignment with the business strategy.
- Respond to governance requirements in line with board direction.

Process

- Define how business requirements are translated in service offerings.
- Define the strategy to deliver service offerings.
- Contribute to the management of the portfolio of IT-enabled business investments.
- Establish clarity regarding the business impact of risks on IT objectives and resources.
- Provide transparency and understanding of IT costs, benefits, strategy, policies and service levels.

Activities

- Engaging with business and senior management in aligning IT strategic planning with current and future business needs
- Understanding current IT capabilities
- Providing for a prioritisation scheme for the business objectives that quantifies the business requirements
- Translating IT strategic planning into tactical plans

Metrics (IT)

- Degree of approval of business owners of the IT strategic/tactical plans
- Degree of compliance with business and governance requirements
- Level of business satisfaction with the current state (number, scope, etc.) of the project and applications portfolio

Metrics (Process)

- Percent of IT objectives in the IT strategic plan that support the strategic business plan
- Percent of IT initiatives in the IT tactical plan that support the tactical business plans
- Percent of IT projects in the IT project portfolio that can be directly traced back to the IT tactical plans

Metrics (Activities)

- Delay between updates of business strategic/tactical plans and updates of IT strategic/tactical plans
- Percent of strategic/tactical IT plans meetings where business representatives have actively participated
- Delay between updates of IT strategic plan and updates of IT tactical plans
- Percent of tactical IT plans complying with the predefined structure/contents of those plans
- Percent of IT initiatives/projects championed by business owners

Maturity Model

P01 Define a Strategic IT Plan

Management of the process of *Define a strategic IT plan* that satisfies the business requirement for IT of *sustaining or extending the business strategy and governance requirements whilst being transparent about benefits, costs and risks* is:

0 Non-existent when
IT strategic planning is not performed. There is no management awareness that IT strategic planning is needed to support business goals.

1 Initial/*Ad Hoc* when
The need for IT strategic planning is known by IT management. IT planning is performed on an as-needed basis in response to a specific business requirement. IT strategic planning is occasionally discussed at IT management meetings. The alignment of business requirements, applications and technology takes place reactively rather than by an organisationwide strategy. The strategic risk position is identified informally on a project-by-project basis.

2 Repeatable but Intuitive when
IT strategic planning is shared with business management on an as-needed basis. Updating of the IT plans occurs in response to requests by management. Strategic decisions are driven on a project-by-project basis without consistency with an overall organisation strategy. The risks and user benefits of major strategic decisions are recognised in an intuitive way.

3 Defined when
A policy defines when and how to perform IT strategic planning. IT strategic planning follows a structured approach that is documented and known to all staff. The IT planning process is reasonably sound and ensures that appropriate planning is likely to be performed. However, discretion is given to individual managers with respect to implementation of the process, and there are no procedures to examine the process. The overall IT strategy includes a consistent definition of risks that the organisation is willing to take as an innovator or follower. The IT financial, technical and human resources strategies increasingly influence the acquisition of new products and technologies. IT strategic planning is discussed at business management meetings.

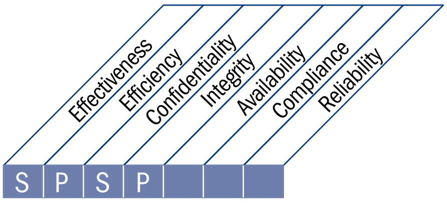
4 Managed and Measurable when
IT strategic planning is standard practice and exceptions would be noticed by management. IT strategic planning is a defined management function with senior-level responsibilities. Management is able to monitor the IT strategic planning process, make informed decisions based on it and measure its effectiveness. Both short-range and long-range IT planning occurs and is cascaded down into the organisation, with updates done as needed. The IT strategy and organisationwide strategy are increasingly becoming more co-ordinated by addressing business processes and value-added capabilities and leveraging the use of applications and technologies through business process re-engineering. There is a well-defined process for determining the usage of internal and external resources required in system development and operations.

5 Optimised when
IT strategic planning is a documented, living process; is continuously considered in business goal setting; and results in discernible business value through investments in IT. Risk and value-added considerations are continuously updated in the IT strategic planning process. Realistic long-range IT plans are developed and constantly updated to reflect changing technology and business-related developments. Benchmarking against well-understood and reliable industry norms takes place and is integrated with the strategy formulation process. The strategic plan includes how new technology developments can drive the creation of new business capabilities and improve the competitive advantage of the organisation.

Process Description

PO2 Define the Information Architecture

The information systems function creates and regularly updates a business information model and defines the appropriate systems to optimise the use of this information. This encompasses the development of a corporate data dictionary with the organisation's data syntax rules, data classification scheme and security levels. This process improves the quality of management decision making by making sure that reliable and secure information is provided, and it enables rationalising information systems resources to appropriately match business strategies. This IT process is also needed to increase accountability for the integrity and security of data and to enhance the effectiveness and control of sharing information across applications and entities.



Control over the IT process of

Define the information architecture

that satisfies the business requirement for IT of

being agile in responding to requirements, to provide reliable and consistent information and to seamlessly integrate applications into business processes

by focusing on

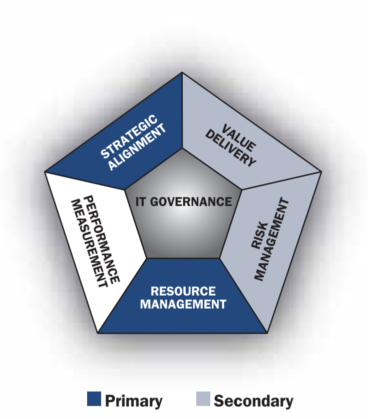
the establishment of an enterprise data model that incorporates a data classification scheme to ensure the integrity and consistency of all data

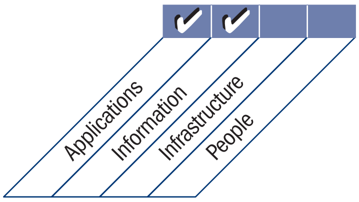
is achieved by

- Assuring the accuracy of the information architecture and data model
- Assigning data ownership
- Classifying information using an agreed-upon classification scheme

and is measured by

- Percent of redundant/duplicate data elements
- Percent of applications not complying with the information architecture methodology used by the enterprise
- Frequency of data validation activities





Control Objectives

PO2 Define the Information Architecture

PO2.1 Enterprise Information Architecture Model
Establish and maintain an enterprise information model to enable applications development and decision-supporting activities, consistent with IT plans as described in PO1. The model should facilitate the optimal creation, use and sharing of information by the business in a way that maintains integrity and is flexible, functional, cost-effective, timely, secure and resilient to failure.

PO2.2 Enterprise Data Dictionary and Data Syntax Rules
Maintain an enterprise data dictionary that incorporates the organisation's data syntax rules. This dictionary should enable the sharing of data elements amongst applications and systems, promote a common understanding of data amongst IT and business users, and prevent incompatible data elements from being created.

PO2.3 Data Classification Scheme
Establish a classification scheme that applies throughout the enterprise, based on the criticality and sensitivity (e.g., public, confidential, top secret) of enterprise data. This scheme should include details about data ownership; definition of appropriate security levels and protection controls; and a brief description of data retention and destruction requirements, criticality and sensitivity. It should be used as the basis for applying controls such as access controls, archiving or encryption.

PO2.4 Integrity Management
Define and implement procedures to ensure the integrity and consistency of all data stored in electronic form, such as databases, data warehouses and data archives.

Management Guidelines

PO2 Define the Information Architecture

From	Inputs
PO1	Strategic and tactical IT plans
AI1	Business requirements feasibility study
AI7	Post-implementation review
DS3	Performance and capacity information
ME1	Performance input to IT planning

Outputs	To						
Data classification scheme	AI2						
Optimised business systems plan	PO3	AI2					
Data dictionary	AI2	DS11					
Information architecture	PO3	DS5					
Assigned data classifications	DS1	DS4	DS5	DS11	DS12		
Classification procedures and tools	*						

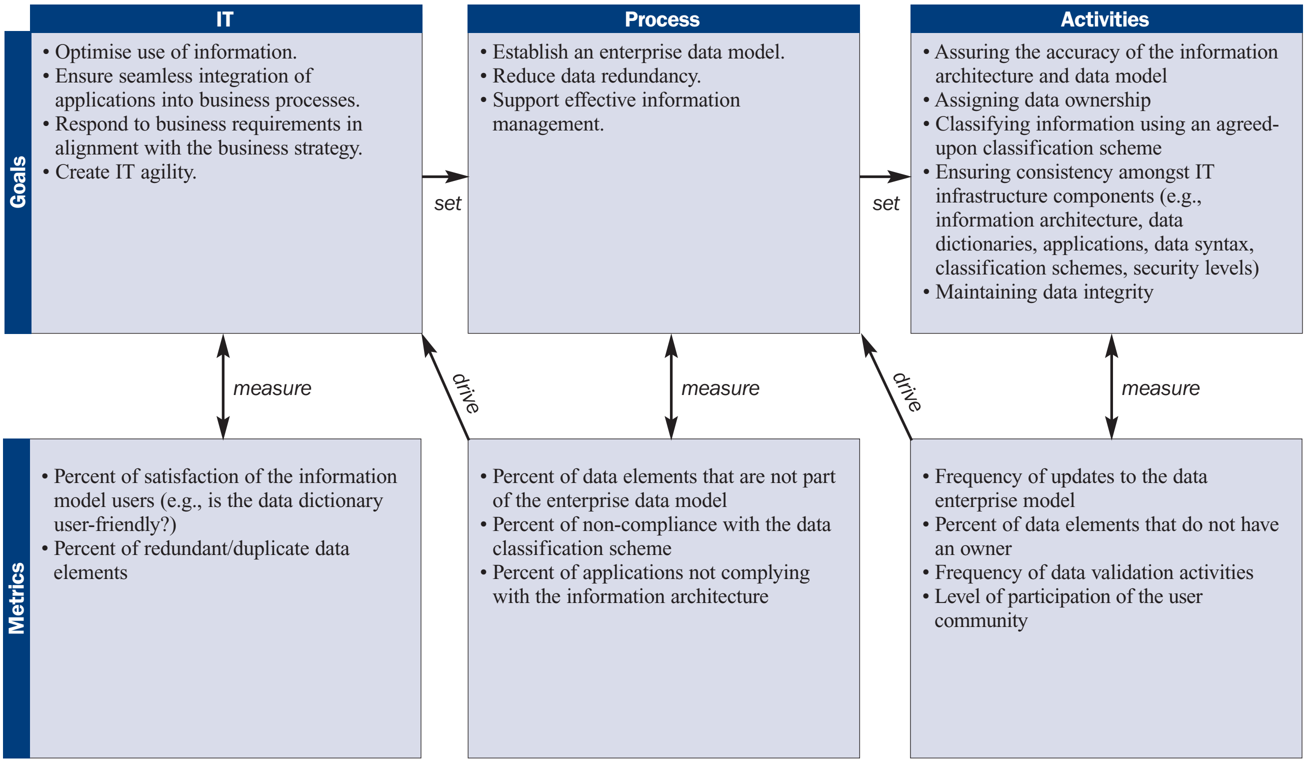
* Outputs to outside CobiT

RACI Chart

Activities	CEO	CFO	Business Executive	CIO	Business Process Owner	Head Operations	Chief Architect	Head Development	Head IT Administration	PMO	Compliance, Audit, Risk and Security
Create and maintain corporate/enterprise information model.		C	I	A	C		R	C	C		C
Create and maintain corporate data dictionary(ies).				I	C		A/R	R			C
Establish and maintain a data classification scheme.	I	C	A	C	C	I	C	C			R
Provide data owners with procedures and tools for classifying information systems.	I	C	A	C	C	I	C	C			R
Utilise the information model, data dictionary and classification scheme to plan optimised business systems.	C	C	I	A	C		R	C			I

A **RACI** chart identifies who is **R**esponsible, **A**ccountable, **C**onsulted and/or **I**nformed.

Goals and Metrics



IT

Goals:
- Optimise use of information.
- Ensure seamless integration of applications into business processes.
- Respond to business requirements in alignment with the business strategy.
- Create IT agility.

Metrics:
- Percent of satisfaction of the information model users (e.g., is the data dictionary user-friendly?)
- Percent of redundant/duplicate data elements

Process

Goals:
- Establish an enterprise data model.
- Reduce data redundancy.
- Support effective information management.

Metrics:
- Percent of data elements that are not part of the enterprise data model
- Percent of non-compliance with the data classification scheme
- Percent of applications not complying with the information architecture

Activities

Goals:
- Assuring the accuracy of the information architecture and data model
- Assigning data ownership
- Classifying information using an agreed-upon classification scheme
- Ensuring consistency amongst IT infrastructure components (e.g., information architecture, data dictionaries, applications, data syntax, classification schemes, security levels)
- Maintaining data integrity

Metrics:
- Frequency of updates to the data enterprise model
- Percent of data elements that do not have an owner
- Frequency of data validation activities
- Level of participation of the user community

Maturity Model

PO2 Define the Information Architecture

Management of the process of *Define the information architecture* that satisfies the business requirement for IT of *being agile in responding to requirements, to provide reliable and consistent information, and to seamlessly integrate applications into business processes* is:

0 Non-existent when
There is no awareness of the importance of the information architecture for the organisation. The knowledge, expertise and responsibilities necessary to develop this architecture do not exist in the organisation.

1 Initial/*Ad Hoc* when
Management recognises the need for an information architecture. Development of some components of an information architecture is occurring on an *ad hoc* basis. The definitions address data, rather than information, and are driven by application software vendor offerings. There is inconsistent and sporadic communication of the need for an information architecture.

2 Repeatable but Intuitive when
An information architecture process emerges and similar, though informal and intuitive, procedures are followed by different individuals within the organisation. Staff obtain their skills in building the information architecture through hands-on experience and repeated application of techniques. Tactical requirements drive the development of information architecture components by individual staff members.

3 Defined when
The importance of the information architecture is understood and accepted, and responsibility for its delivery is assigned and clearly communicated. Related procedures, tools and techniques, although not sophisticated, have been standardised and documented and are part of informal training activities. Basic information architecture policies have been developed, including some strategic requirements, but compliance with policies, standards and tools is not consistently enforced. A formally defined data administration function is in place, setting organisationwide standards, and is beginning to report on the delivery and use of the information architecture. Automated tools are beginning to be employed, but the processes and rules used are defined by database software vendor offerings. A formal training plan has been developed, but formalised training is still based on individual initiatives.

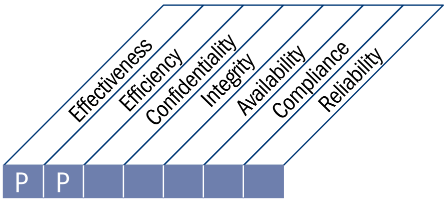
4 Managed and Measurable when
The development and enforcement of the information architecture are fully supported by formal methods and techniques. Accountability for the performance of the architecture development process is enforced and success of the information architecture is being measured. Supporting automated tools are widespread, but are not yet integrated. Basic metrics have been identified and a measurement system is in place. The information architecture definition process is proactive and focused on addressing future business needs. The data administration organisation is actively involved in all application development efforts, to ensure consistency. An automated repository is fully implemented. More complex data models are being implemented to leverage the information content of the databases. Executive information systems and decision support systems are leveraging the available information.

5 Optimised when
The information architecture is consistently enforced at all levels. The value of the information architecture to the business is continually stressed. IT personnel have the expertise and skills necessary to develop and maintain a robust and responsive information architecture that reflects all the business requirements. The information provided by the information architecture is consistently and extensively applied. Extensive use is made of industry good practices in the development and maintenance of the information architecture, including a continuous improvement process. The strategy for leveraging information through data warehousing and data mining technologies is defined. The information architecture is continuously improving and takes into consideration non-traditional information on processes, organisations and systems.

Process Description

PO3 Determine Technological Direction

The information services function determines the technology direction to support the business. This requires the creation of a technological infrastructure plan and an architecture board that sets and manages clear and realistic expectations of what technology can offer in terms of products, services and delivery mechanisms. The plan is regularly updated and encompasses aspects such as systems architecture, technological direction, acquisition plans, standards, migration strategies and contingency. This enables timely responses to changes in the competitive environment, economies of scale for information systems staffing and investments, as well as improved interoperability of platforms and applications.



Plan and Organise
Acquire and Implement
Deliver and Support
Monitor and Evaluate

Control over the IT process of

Determine technological direction

that satisfies the business requirement for IT of

having stable, cost-effective, integrated and standard application systems, resources and capabilities that meet current and future business requirements

by focusing on

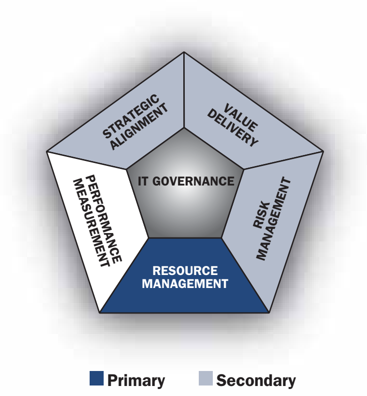
defining and implementing a technology infrastructure plan, architecture and standards that recognise and leverage technology opportunities

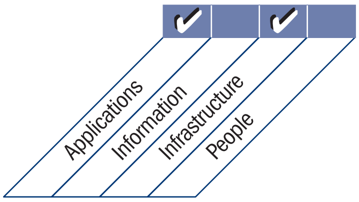
is achieved by

- Establishing a forum to guide architecture and verify compliance
- Establishing the technology infrastructure plan balanced against cost, risk and requirements
- Defining the technology infrastructure standards based on information architecture requirements

and is measured by

- Number and type of deviations from the technology infrastructure plan
- Frequency of the technology infrastructure plan review/update
- Number of technology platforms by function across the enterprise





Control Objectives

PO3 Determine Technological Direction

PO3.1 Technological Direction Planning
Analyse existing and emerging technologies, and plan which technological direction is appropriate to realise the IT strategy and the business systems architecture. Also identify in the plan which technologies have the potential to create business opportunities. The plan should address systems architecture, technological direction, migration strategies and contingency aspects of infrastructure components.

PO3.2 Technology Infrastructure Plan
Create and maintain a technology infrastructure plan that is in accordance with the IT strategic and tactical plans. The plan should be based on the technological direction and include contingency arrangements and direction for acquisition of technology resources. It should consider changes in the competitive environment, economies of scale for information systems staffing and investments, and improved interoperability of platforms and applications.

PO3.3 Monitor Future Trends and Regulations
Establish a process to monitor the business sector, industry, technology, infrastructure, legal and regulatory environment trends. Incorporate the consequences of these trends into the development of the IT technology infrastructure plan.

PO3.4 Technology Standards
To provide consistent, effective and secure technological solutions enterprisewide, establish a technology forum to provide technology guidelines, advice on infrastructure products and guidance on the selection of technology, and measure compliance with these standards and guidelines. This forum should direct technology standards and practices based on their business relevance, risks and compliance with external requirements.

PO3.5 IT Architecture Board
Establish an IT architecture board to provide architecture guidelines and advice on their application, and to verify compliance. This entity should direct IT architecture design, ensuring that it enables the business strategy and considers regulatory compliance and continuity requirements. This is related/linked to PO2 *Define the information architecture*.

Management Guidelines

PO3 Determine Technological Direction

From	Inputs
PO1	Strategic and tactical IT plans
PO2	Optimised business systems plan, information architecture
AI3	Updates for technology standards
DS3	Performance and capacity information

Outputs	To						
Technology opportunities	AI3						
Technology standards	AI1	AI3	AI7	DS5			
Regular 'state of technology' updates	AI1	AI2	AI3				
Technology infrastructure plan	AI3						
Infrastructure requirements	PO5						

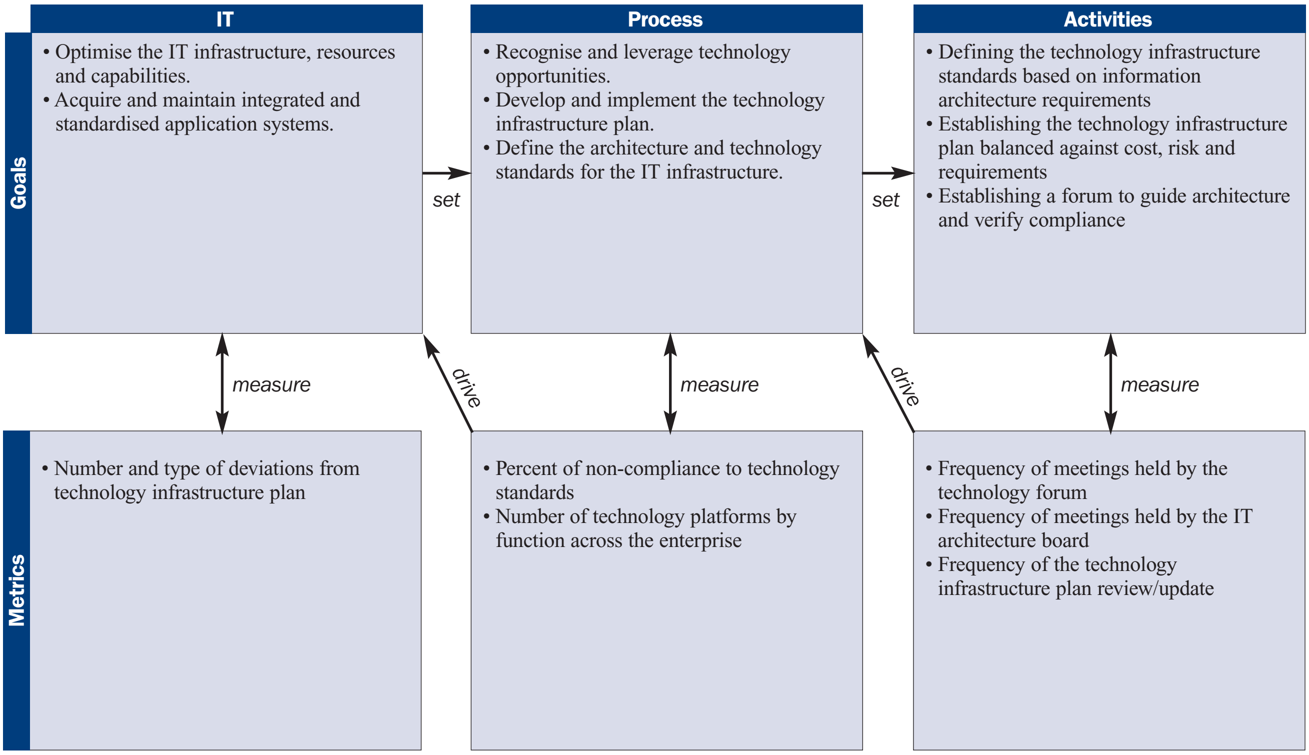
RACI Chart

Functions

Activities	CEO	CFO	Business Executive	CIO	Business Process Owner	Head Operations	Chief Architect	Head Development	Head IT Administration	PMO	Compliance, Audit, Risk and Security
Create and maintain a technology infrastructure plan.		I	I	A		C	R	C	C		C
Create and maintain technology standards.				A		C	R	C	I	I	I
Publish technology standards.		I	I	A		I	R	I	I	I	I
Monitor technology evolution.		I	I	A		C	R	C		C	C
Define (future) (strategic) use of new technology.		C	C	A		C	R	C		C	C

A **RACI** chart identifies who is **R**esponsible, **A**ccountable, **C**onsulted and/or **I**nformed.

Goals and Metrics



Goals – IT
- Optimise the IT infrastructure, resources and capabilities.
- Acquire and maintain integrated and standardised application systems.

Goals – Process
- Recognise and leverage technology opportunities.
- Develop and implement the technology infrastructure plan.
- Define the architecture and technology standards for the IT infrastructure.

Goals – Activities
- Defining the technology infrastructure standards based on information architecture requirements
- Establishing the technology infrastructure plan balanced against cost, risk and requirements
- Establishing a forum to guide architecture and verify compliance

Metrics – IT
- Number and type of deviations from technology infrastructure plan

Metrics – Process
- Percent of non-compliance to technology standards
- Number of technology platforms by function across the enterprise

Metrics – Activities
- Frequency of meetings held by the technology forum
- Frequency of meetings held by the IT architecture board
- Frequency of the technology infrastructure plan review/update

Maturity Model

PO3 Determine Technological Direction

Management of the process of *Determine technological direction* that satisfies the business requirement for IT of *having stable, cost-effective, integrated and standard application systems, resources and capabilities that meet current and future business requirements* is:

0 Non-existent when
There is no awareness of the importance of technology infrastructure planning for the entity. The knowledge and expertise necessary to develop such a technology infrastructure plan do not exist. There is a lack of understanding that planning for technological change is critical to effectively allocate resources.

1 Initial/*Ad Hoc* when
Management recognises the need for technology infrastructure planning. Technology component developments and emerging technology implementations are *ad hoc* and isolated. There is a reactive and operationally focused approach to infrastructure planning. Technology directions are driven by the often contradictory product evolution plans of hardware, systems software and applications software vendors. Communication of the potential impact of changes in technology is inconsistent.

2 Repeatable but Intuitive when
The need for and importance of technology planning are communicated. Planning is tactical and focused on generating solutions to technical problems, rather than on the use of technology to meet business needs. Evaluation of technological changes is left to different individuals who follow intuitive, but similar, processes. People obtain their skills in technology planning through hands-on learning and repeated application of techniques. Common techniques and standards are emerging for the development of infrastructure components.

3 Defined when
Management is aware of the importance of the technology infrastructure plan. The technology infrastructure plan development process is reasonably sound and aligned with the IT strategic plan. There is a defined, documented and well-communicated technology infrastructure plan, but it is inconsistently applied. The technology infrastructure direction includes an understanding of where the organisation wants to lead or lag in the use of technology, based on risks and alignment with the organisation's strategy. Key vendors are selected based on the understanding of their long-term technology and product development plans, consistent with the organisation's direction. Formal training and communication of roles and responsibilities exist.

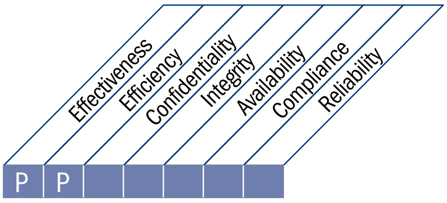
4 Managed and Measurable when
Management ensures the development and maintenance of the technology infrastructure plan. IT staff members have the expertise and skills necessary to develop a technology infrastructure plan. The potential impact of changing and emerging technologies is taken into account. Management can identify deviations from the plan and anticipate problems. Responsibility for the development and maintenance of a technology infrastructure plan has been assigned. The process of developing the technology infrastructure plan is sophisticated and responsive to change. Internal good practices have been introduced into the process. The human resources strategy is aligned with the technology direction, to ensure that IT staff members can manage technology changes. Migration plans for introducing new technologies are defined. Outsourcing and partnering are being leveraged to access necessary expertise and skills. Management has analysed the acceptance of risk regarding the lead or lag use of technology in developing new business opportunities or operational efficiencies.

5 Optimised when
A research function exists to review emerging and evolving technologies and benchmark the organisation against industry norms. The direction of the technology infrastructure plan is guided by industry and international standards and developments, rather than driven by technology vendors. The potential business impact of technological change is reviewed at senior management levels. There is formal executive approval of new and changed technological directions. The entity has a robust technology infrastructure plan that reflects the business requirements, is responsive and can be modified to reflect changes in the business environment. There is a continuous and enforced process in place to improve the technology infrastructure plan. Industry good practices are extensively used in determining the technological direction.

Process Description

PO4 Define the IT Processes, Organisation and Relationships

An IT organisation is defined by considering requirements for staff, skills, functions, accountability, authority, roles and responsibilities, and supervision. This organisation is embedded into an IT process framework that ensures transparency and control as well as the involvement of senior executives and business management. A strategy committee ensures board oversight of IT, and one or more steering committees in which business and IT participate determine the prioritisation of IT resources in line with business needs. Processes, administrative policies and procedures are in place for all functions, with specific attention to control, quality assurance, risk management, information security, data and systems ownership, and segregation of duties. To ensure timely support of business requirements, IT is to be involved in relevant decision processes.



Plan and Organise
Acquire and Implement
Deliver and Support
Monitor and Evaluate

Control over the IT process of

Define the IT processes, organisation and relationships

that satisfies the business requirement for IT of

being agile in responding to the business strategy whilst complying with governance requirements and providing defined and competent points of contact

by focusing on

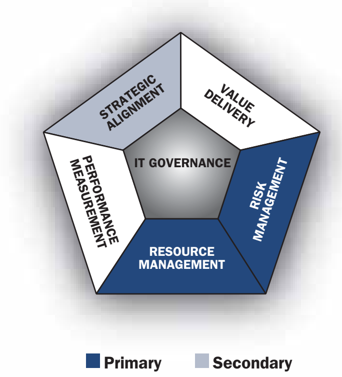
establishing transparent, flexible and responsive IT organisational structures and defining and implementing IT processes with owners, roles and responsibilities integrated into business and decision processes

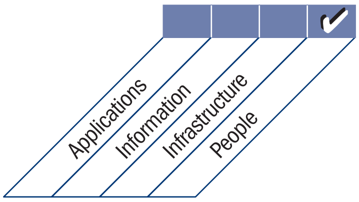
is achieved by

- Defining an IT process framework
- Establishing appropriate organisational bodies and structure
- Defining roles and responsibilities

and is measured by

- Percent of roles with documented position and authority descriptions
- Number of business units/processes not supported by the IT organisation that should be supported, according to the strategy
- Number of core IT activities outside of the IT organisation that are not approved or are not subject to IT organisational standards





Control Objectives

PO4 Define the IT Processes, Organisation and Relationships

PO4.1 IT Process Framework

Define an IT process framework to execute the IT strategic plan. This framework should include an IT process structure and relationships (e.g., to manage process gaps and overlaps), ownership, maturity, performance measurement, improvement, compliance, quality targets and plans to achieve them. It should provide integration amongst the processes that are specific to IT, enterprise portfolio management, business processes and business change processes. The IT process framework should be integrated into a quality management system (QMS) and the internal control framework.

PO4.2 IT Strategy Committee

Establish an IT strategy committee at the board level. This committee should ensure that IT governance, as part of enterprise governance, is adequately addressed; advise on strategic direction; and review major investments on behalf of the full board.

PO4.3 IT Steering Committee

Establish an IT steering committee (or equivalent) composed of executive, business and IT management to:

- Determine prioritisation of IT-enabled investment programmes in line with the enterprise's business strategy and priorities
- Track status of projects and resolve resource conflict
- Monitor service levels and service improvements

PO4.4 Organisational Placement of the IT Function

Place the IT function in the overall organisational structure with a business model contingent on the importance of IT within the enterprise, specifically its criticality to business strategy and the level of operational dependence on IT. The reporting line of the CIO should be commensurate with the importance of IT within the enterprise.

PO4.5 IT Organisational Structure

Establish an internal and external IT organisational structure that reflects business needs. In addition, put a process in place for periodically reviewing the IT organisational structure to adjust staffing requirements and sourcing strategies to meet expected business objectives and changing circumstances.

PO4.6 Establishment of Roles and Responsibilities

Establish and communicate roles and responsibilities for IT personnel and end users that delineate between IT personnel and end-user authority, responsibilities and accountability for meeting the organisation's needs.

PO4.7 Responsibility for IT Quality Assurance

Assign responsibility for the performance of the quality assurance (QA) function and provide the QA group with appropriate QA systems, controls and communications expertise. Ensure that the organisational placement and the responsibilities and size of the QA group satisfy the requirements of the organisation.

PO4.8 Responsibility for Risk, Security and Compliance

Embed ownership and responsibility for IT-related risks within the business at an appropriate senior level. Define and assign roles critical for managing IT risks, including the specific responsibility for information security, physical security and compliance. Establish risk and security management responsibility at the enterprise level to deal with organisationwide issues. Additional security management responsibilities may need to be assigned at a system-specific level to deal with related security issues. Obtain direction from senior management on the appetite for IT risk and approval of any residual IT risks.

PO4.9 Data and System Ownership

Provide the business with procedures and tools, enabling it to address its responsibilities for ownership of data and information systems. Owners should make decisions about classifying information and systems and protecting them in line with this classification.

PO4.10 Supervision

Implement adequate supervisory practices in the IT function to ensure that roles and responsibilities are properly exercised, to assess whether all personnel have sufficient authority and resources to execute their roles and responsibilities, and to generally review KPIs.

PO4.11 Segregation of Duties

Implement a division of roles and responsibilities that reduces the possibility for a single individual to compromise a critical process. Make sure that personnel are performing only authorised duties relevant to their respective jobs and positions.

PO4.12 IT Staffing
Evaluate staffing requirements on a regular basis or upon major changes to the business, operational or IT environments to ensure that the IT function has sufficient resources to adequately and appropriately support the business goals and objectives.

PO4.13 Key IT Personnel
Define and identify key IT personnel (e.g., replacements/backup personnel), and minimise reliance on a single individual performing a critical job function.

PO4.14 Contracted Staff Policies and Procedures
Ensure that consultants and contract personnel who support the IT function know and comply with the organisation's policies for the protection of the organisation's information assets such that they meet agreed-upon contractual requirements.

PO4.15 Relationships
Establish and maintain an optimal co-ordination, communication and liaison structure between the IT function and various other interests inside and outside the IT function, such as the board, executives, business units, individual users, suppliers, security officers, risk managers, the corporate compliance group, outsourcers and offsite management.

Page intentionally left blank

Management Guidelines

PO4 Define the IT Processes, Organisation and Relationships

From	Inputs
PO1	Strategic and tactical plans
PO7	IT human resources policy and procedures, IT skills matrix, job descriptions
PO8	Quality improvement actions
PO9	IT-related risk remedial action plans
ME1	Remedial action plans
ME2	Report on effectiveness of IT controls
ME3	Catalogue of legal and regulatory requirements related to IT service delivery
ME4	Process framework improvements

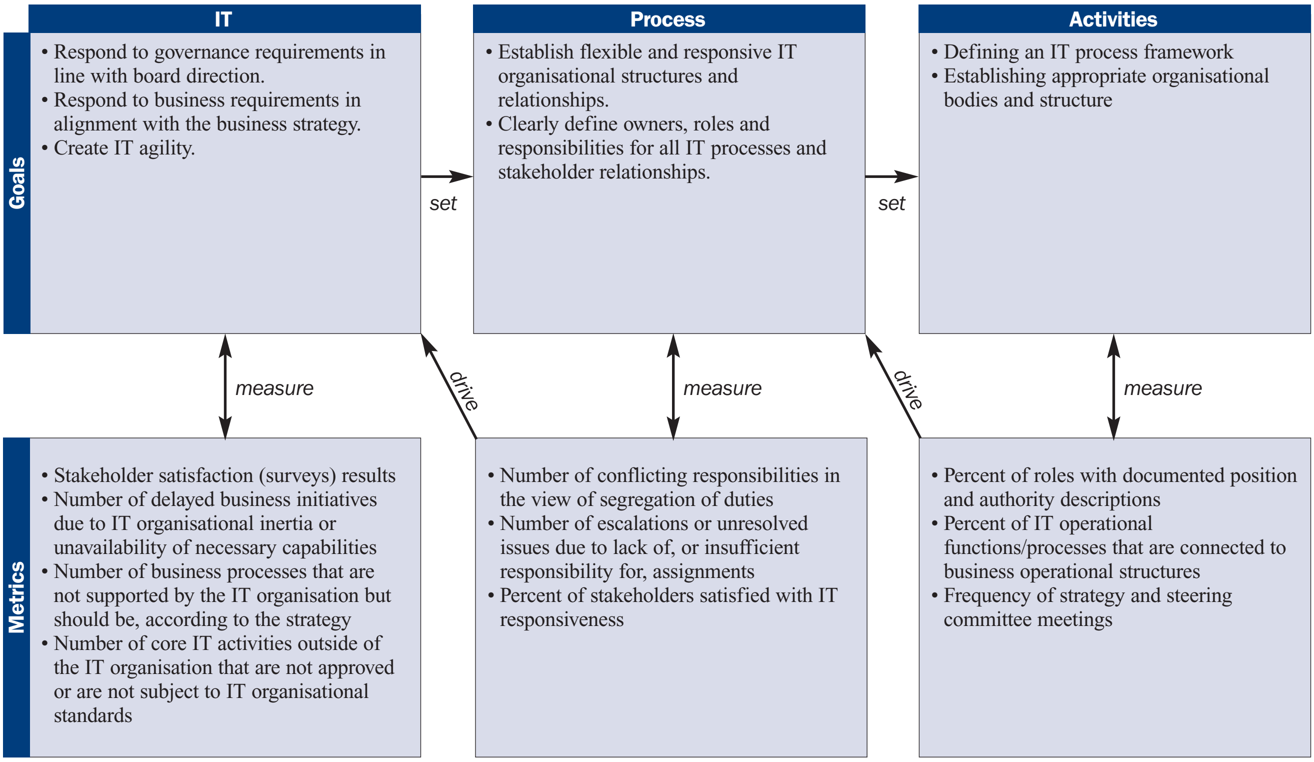
Outputs	To						
IT process framework	ME4						
Documented system owners	AI7	DS6					
IT organisation and relationships	PO7						
IT process framework, documented roles and responsibilities	ALL						
Document roles and responsibilities	PO7						

RACI Chart

Activities \ Functions	CEO	CFO	Business Executive	CIO	Business Process Owner	Head Operations	Chief Architect	Head Development	Head IT Administration	PMO	Compliance, Audit, Risk and Security
Establish IT organisational structure, including committees and linkages to the stakeholders and vendors.	C	C	C	A		C	C	C	R	C	I
Design an IT process framework.	C	C	C	A		C	C	C	R	C	C
Identify system owners.		C	C	A	C	R	I	I	I	I	I
Identify data owners.		I	A	C	C	I	R	I	I	I	C
Establish and implement IT roles and responsibilities, including supervision and segregation of duties.		I	I	A	I	C	C	C	R	C	C

A **RACI** chart identifies who is **R**esponsible, **A**ccountable, **C**onsulted and/or **I**nformed.

Goals and Metrics



IT – Goals

- Respond to governance requirements in line with board direction.
- Respond to business requirements in alignment with the business strategy.
- Create IT agility.

Process – Goals

- Establish flexible and responsive IT organisational structures and relationships.
- Clearly define owners, roles and responsibilities for all IT processes and stakeholder relationships.

Activities – Goals

- Defining an IT process framework
- Establishing appropriate organisational bodies and structure

IT – Metrics

- Stakeholder satisfaction (surveys) results
- Number of delayed business initiatives due to IT organisational inertia or unavailability of necessary capabilities
- Number of business processes that are not supported by the IT organisation but should be, according to the strategy
- Number of core IT activities outside of the IT organisation that are not approved or are not subject to IT organisational standards

Process – Metrics

- Number of conflicting responsibilities in the view of segregation of duties
- Number of escalations or unresolved issues due to lack of, or insufficient responsibility for, assignments
- Percent of stakeholders satisfied with IT responsiveness

Activities – Metrics

- Percent of roles with documented position and authority descriptions
- Percent of IT operational functions/processes that are connected to business operational structures
- Frequency of strategy and steering committee meetings

Maturity Model

PO4 Define the IT Processes, Organisation and Relationships

Management of the process of *Define the IT processes, organisation and relationships* that satisfies the business requirement for IT of *being agile in responding to the business strategy whilst complying with governance requirements and providing defined and competent points of contact* is:

0 Non-existent when
The IT organisation is not effectively established to focus on the achievement of business objectives.

1 Initial/*Ad Hoc* when
IT activities and functions are reactive and inconsistently implemented. IT is involved in business projects only in later stages. The IT function is considered a support function, without an overall organisation perspective. There is an implicit understanding of the need for an IT organisation; however, roles and responsibilities are neither formalised nor enforced.

2 Repeatable but Intuitive when
The IT function is organised to respond tactically, but inconsistently, to customer needs and vendor relationships. The need for a structured organisation and vendor management is communicated, but decisions are still dependent on the knowledge and skills of key individuals. There is an emergence of common techniques to manage the IT organisation and vendor relationships.

3 Defined when
Defined roles and responsibilities for the IT organisation and third parties exist. The IT organisation is developed, documented, communicated and aligned with the IT strategy. The internal control environment is defined. There is formalisation of relationships with other parties, including steering committees, internal audit and vendor management. The IT organisation is functionally complete. There are definitions of the functions to be performed by IT personnel and those to be performed by users. Essential IT staffing requirements and expertise are defined and satisfied. There is a formal definition of relationships with users and third parties. The division of roles and responsibilities is defined and implemented.

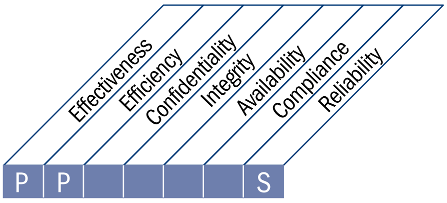
4 Managed and Measurable when
The IT organisation proactively responds to change and includes all roles necessary to meet business requirements. IT management, process ownership, accountability and responsibility are defined and balanced. Internal good practices have been applied in the organisation of the IT functions. IT management has the appropriate expertise and skills to define, implement and monitor the preferred organisation and relationships. Measurable metrics to support business objectives and user-defined critical success factors (CSFs) are standardised. Skill inventories are available to support project staffing and professional development. The balance between the skills and resources available internally and those needed from external organisations is defined and enforced. The IT organisational structure appropriately reflects the business needs by providing services aligned with strategic business processes, rather than with isolated technologies.

5 Optimised when
The IT organisational structure is flexible and adaptive. Industry good practices are deployed. There is extensive use of technology to assist in monitoring the performance of the IT organisation and processes. Technology is leveraged in line to support the complexity and geographic distribution of the organisation. There is a continuous improvement process in place.

Process Description

PO5 Manage the IT Investment

A framework is established and maintained to manage IT-enabled investment programmes and that encompasses cost, benefits, prioritisation within budget, a formal budgeting process and management against the budget. Stakeholders are consulted to identify and control the total costs and benefits within the context of the IT strategic and tactical plans, and initiate corrective action where needed. The process fosters partnership between IT and business stakeholders; enables the effective and efficient use of IT resources; and provides transparency and accountability into the total cost of ownership (TCO), the realisation of business benefits and the ROI of IT-enabled investments.



Control over the IT process of

Manage the IT investment

that satisfies the business requirement for IT of

continuously and demonstrably improving IT's cost-efficiency and its contribution to business profitability with integrated and standardised services that satisify end-user expectations

by focusing on

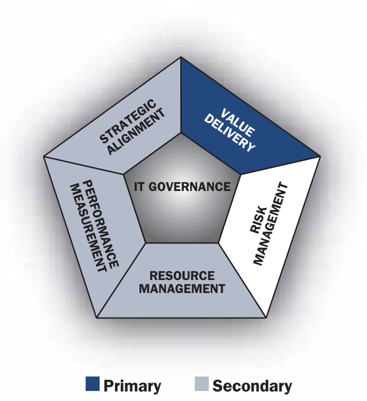
effective and efficient IT investment and portfolio decisions, and by setting and tracking IT budgets in line with IT strategy and investment decisions

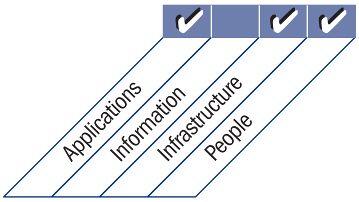
is achieved by

- Forecasting and allocating budgets
- Defining formal investment criteria (ROI, payback period, net present value [NPV])
- Measuring and assessing business value against forecast

and is measured by

- Percent of reduction of the unit cost of the delivered IT services
- Percent of budget deviation value compared to the total budget
- Percent of IT expenditure expressed in business value drivers (e.g., sales/services increase due to increased connectivity)





CONTROL OBJECTIVES

PO5 Manage the IT Investment

PO5.1 Financial Management Framework
Establish and maintain a financial framework to manage the investment and cost of IT assets and services through portfolios of IT-enabled investments, business cases and IT budgets.

PO5.2 Prioritisation Within IT Budget
Implement a decision-making process to prioritise the allocation of IT resources for operations, projects and maintenance to maximise IT's contribution to optimising the return on the enterprise's portfolio of IT-enabled investment programmes and other IT services and assets.

PO5.3 IT Budgeting
Establish and implement practices to prepare a budget reflecting the priorities established by the enterprise's portfolio of IT-enabled investment programmes, and including the ongoing costs of operating and maintaining the current infrastructure. The practices should support development of an overall IT budget as well as development of budgets for individual programmes, with specific emphasis on the IT components of those programmes. The practices should allow for ongoing review, refinement and approval of the overall budget and the budgets for individual programmes.

PO5.4 Cost Management
Implement a cost management process comparing actual costs to budgets. Costs should be monitored and reported. Where there are deviations, these should be identified in a timely manner and the impact of those deviations on programmes should be assessed. Together with the business sponsor of those programmes, appropriate remedial action should be taken and, if necessary, the programme business case should be updated.

PO5.5 Benefit Management
Implement a process to monitor the benefits from providing and maintaining appropriate IT capabilities. IT's contribution to the business, either as a component of IT-enabled investment programmes or as part of regular operational support, should be identified and documented in a business case, agreed to, monitored and reported. Reports should be reviewed and, where there are opportunities to improve IT's contribution, appropriate actions should be defined and taken. Where changes in IT's contribution impact the programme, or where changes to other related projects impact the programme, the programme business case should be updated.

Management Guidelines

PO5 Manage the IT Investment

From	Inputs
PO1	Strategic plan and tactical IT plans, project and service portfolios
PO3	Infrastructure requirements
PO10	Updated IT project portfolio
AI1	Business requirements feasibility study
AI7	Post-implementation reviews
DS3	Performance and capacity plan (requirements)
DS6	IT financials
ME4	Expected business outcome of IT-enabled business investments

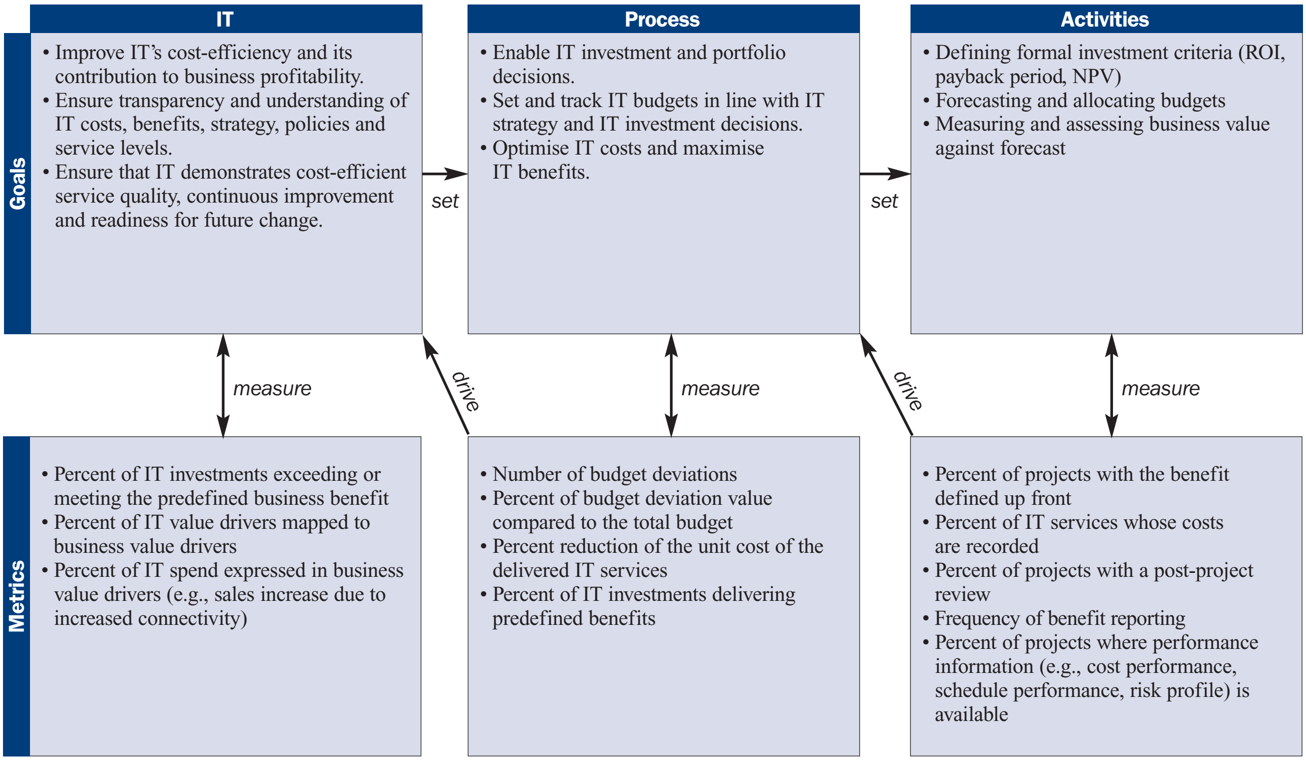
Outputs	To						
Cost-benefit reports	PO1	AI2	DS6	ME1	ME4		
IT budgets	DS6						
Updated IT service portfolio	DS1						
Updated IT project portfolio	PO10						

RACI Chart

Activities	CEO	CFO	Business Executive	CIO	Business Process Owner	Head Operations	Chief Architect	Head Development	Head IT Administration	PMO	Compliance, Audit, Risk and Security
Maintain the programme portfolio.	A	R	R	R	C					I	I
Maintain the project portfolio.	I	C	A/R	A/R	C		C	C		C	I
Maintain the service portfolio.	I	C	A/R	A/R	C	C				C	I
Establish and maintain the IT budgeting process.	I	C	C	A		C	C	C	R	C	
Identify, communicate and monitor IT investments, cost and value to the business.	I	C	C	A/R		C	C	C	R	C	C

A **RACI** chart identifies who is **R**esponsible, **A**ccountable, **C**onsulted and/or **I**nformed.

Goals and Metrics



IT

- Improve IT's cost-efficiency and its contribution to business profitability.
- Ensure transparency and understanding of IT costs, benefits, strategy, policies and service levels.
- Ensure that IT demonstrates cost-efficient service quality, continuous improvement and readiness for future change.

Process

- Enable IT investment and portfolio decisions.
- Set and track IT budgets in line with IT strategy and IT investment decisions.
- Optimise IT costs and maximise IT benefits.

Activities

- Defining formal investment criteria (ROI, payback period, NPV)
- Forecasting and allocating budgets
- Measuring and assessing business value against forecast

- Percent of IT investments exceeding or meeting the predefined business benefit
- Percent of IT value drivers mapped to business value drivers
- Percent of IT spend expressed in business value drivers (e.g., sales increase due to increased connectivity)

- Number of budget deviations
- Percent of budget deviation value compared to the total budget
- Percent reduction of the unit cost of the delivered IT services
- Percent of IT investments delivering predefined benefits

- Percent of projects with the benefit defined up front
- Percent of IT services whose costs are recorded
- Percent of projects with a post-project review
- Frequency of benefit reporting
- Percent of projects where performance information (e.g., cost performance, schedule performance, risk profile) is available

Maturity Model

PO5 Manage the IT Investment

Management of the process of *Manage the IT investment* that satisfies the business requirement for IT of *continuously and demonstrably improving IT's cost-efficiency and its contribution to business profitability with integrated and standardised services that satisfy end-user expectations* is:

0 Non-existent when
There is no awareness of the importance of IT investment selection and budgeting. There is no tracking or monitoring of IT investments and expenditures.

1 Initial/*Ad Hoc* when
The organisation recognises the need for managing the IT investment, but this need is communicated inconsistently. Allocation of responsibility for IT investment selection and budget development is done on an *ad hoc* basis. Isolated implementations of IT investment selection and budgeting occur, with informal documentation. IT investments are justified on an *ad hoc* basis. Reactive and operationally focused budgeting decisions occur.

2 Repeatable but Intuitive when
There is an implicit understanding of the need for IT investment selection and budgeting. The need for a selection and budgeting process is communicated. Compliance is dependent on the initiative of individuals in the organisation. There is an emergence of common techniques to develop components of the IT budget. Reactive and tactical budgeting decisions occur.

3 Defined when
Policies and processes for investment and budgeting are defined, documented and communicated, and cover key business and technology issues. The IT budget is aligned with the strategic IT and business plans. The budgeting and IT investment selection processes are formalised, documented and communicated. Formal training is emerging but is still based primarily on individual initiatives. Formal approval of IT investment selections and budgets is taking place. IT staff members have the expertise and skills necessary to develop the IT budget and recommend appropriate IT investments.

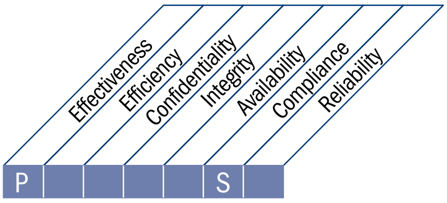
4 Managed and Measurable when
Responsibility and accountability for investment selection and budgeting are assigned to a specific individual. Budget variances are identified and resolved. Formal costing analysis is performed, covering direct and indirect costs of existing operations, as well as proposed investments, considering all costs over a total life cycle. A proactive and standardised process for budgeting is used. The impact of shifting in development and operating costs from hardware and software to systems integration and IT human resources is recognised in the investment plans. Benefits and returns are calculated in financial and non-financial terms.

5 Optimised when
Industry good practices are used to benchmark costs and identify approaches to increase the effectiveness of investments. Analysis of technological developments is used in the investment selection and budgeting process. The investment management process is continuously improved based on lessons learned from the analysis of actual investment performance. Investment decisions incorporate price/performance improvement trends. Funding alternatives are formally investigated and evaluated within the context of the organisation's existing capital structure, using formal evaluation methods. There is proactive identification of variances. An analysis of the long-term cost and benefits of the total life cycle is incorporated in the investment decisions.

Process Description

PO6 Communicate Management Aims and Direction

Management develops an enterprise IT control framework and defines and communicates policies. An ongoing communication programme is implemented to articulate the mission, service objectives, policies and procedures, etc., approved and supported by management. The communication supports achievement of IT objectives and ensures awareness and understanding of business and IT risks, objectives and direction. The process ensures compliance with relevant laws and regulations.



Plan and Organise
Acquire and Implement
Deliver and Support
Monitor and Evaluate

Control over the IT process of

Communicate management aims and direction

that satisfies the business requirement for IT of

supplying accurate and timely information on current and future IT services and associated risks and responsibilities

by focusing on

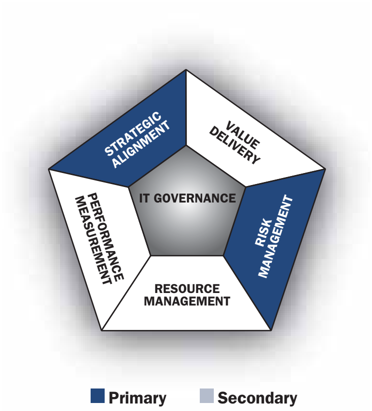
providing accurate, understandable and approved policies, procedures, guidelines and other documentation to stakeholders, embedded in an IT control framework

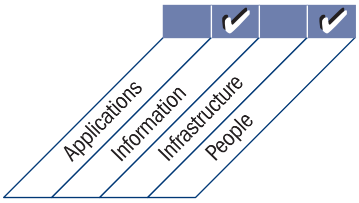
is achieved by

- Defining an IT control framework
- Developing and rolling out IT policies
- Enforcing IT policies

and is measured by

- Number of business disruptions due to IT service disruption
- Percent of stakeholders who understand the enterprise IT control framework
- Percent of stakeholders who are non-compliant with policy





Control Objectives

PO6 Communicate Management Aims and Direction

PO6.1 IT Policy and Control Environment

Define the elements of a control environment for IT, aligned with the enterprise's management philosophy and operating style. These elements should include expectations/requirements regarding delivery of value from IT investments, appetite for risk, integrity, ethical values, staff competence, accountability and responsibility. The control environment should be based on a culture that supports value delivery whilst managing significant risks, encourages cross-divisional co-operation and teamwork, promotes compliance and continuous process improvement, and handles process deviations (including failure) well.

PO6.2 Enterprise IT Risk and Control Framework

Develop and maintain a framework that defines the enterprise's overall approach to IT risk and control and that aligns with the IT policy and control environment and the enterprise risk and control framework.

PO6.3 IT Policies Management

Develop and maintain a set of policies to support IT strategy. These policies should include policy intent; roles and responsibilities; exception process; compliance approach; and references to procedures, standards and guidelines. Their relevance should be confirmed and approved regularly.

PO6.4 Policy, Standard and Procedures Rollout

Roll out and enforce IT policies to all relevant staff, so they are built into and are an integral part of enterprise operations.

PO6.5 Communication of IT Objectives and Direction

Communicate awareness and understanding of business and IT objectives and direction to appropriate stakeholders and users throughout the enterprise.

Management Guidelines

PO6 Communicate Management Aims and Direction

From	Inputs
PO1	Strategic and tactical IT plans, IT project and service portfolios
PO9	IT-related risk management guidelines
ME2	Report on effectiveness of IT controls

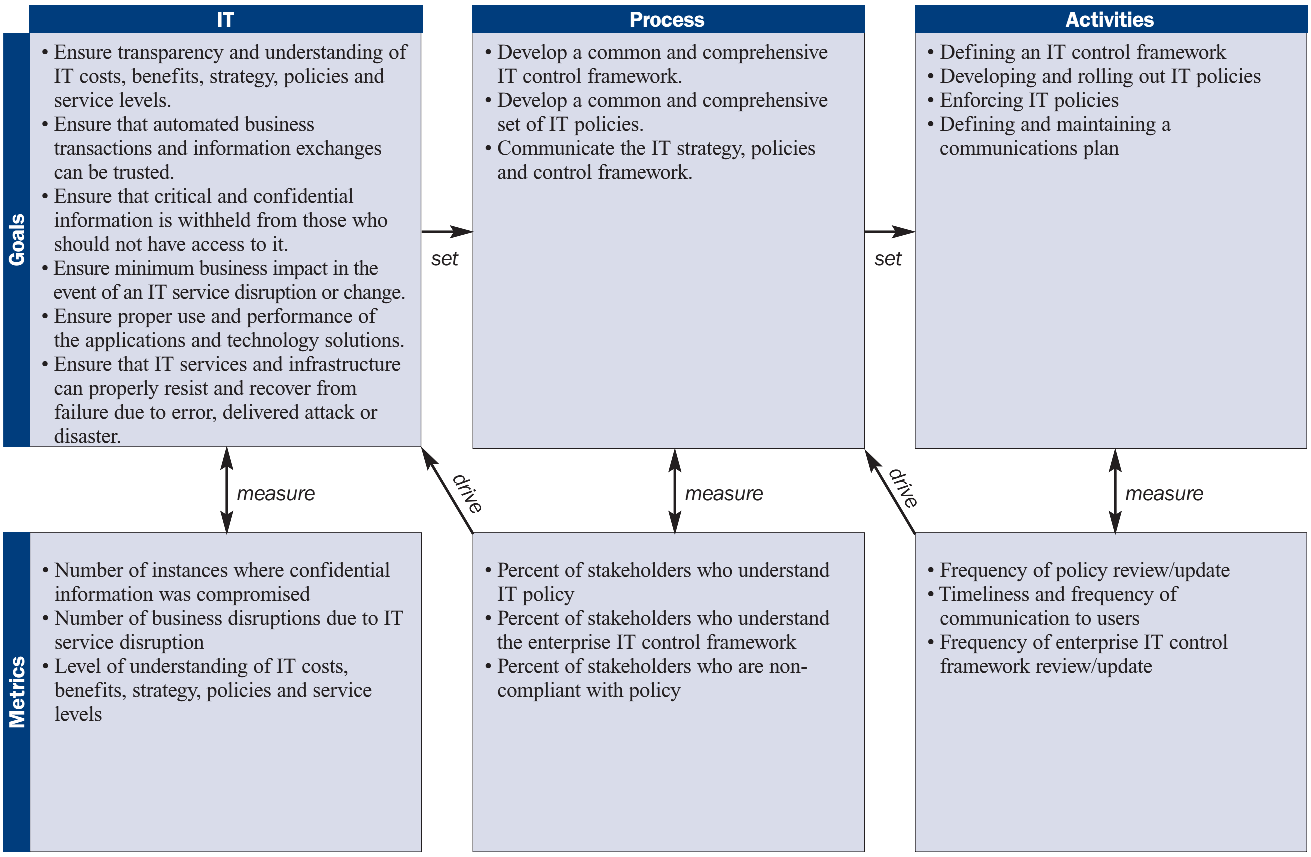
Outputs	To						
Enterprise IT control framework	ALL						
IT policies	ALL						

RACI Chart

Activities	CEO	CFO	Business Executive	CIO	Business Process Owner	Head Operations	Chief Architect	Head Development	Head IT Administration	PMO	Compliance, Audit, Risk and Security
Establish and maintain an IT control environment and framework.	I	C	I	A/R	I	C		C	C		C
Develop and maintain IT policies.	I	I	I	A/R		C	C	C	R		C
Communicate the IT control framework and IT objectives and direction.	I	I	I	A/R					R		C

A **RACI** chart identifies who is **R**esponsible, **A**ccountable, **C**onsulted and/or **I**nformed.

Goals and Metrics



Goals

IT

- Ensure transparency and understanding of IT costs, benefits, strategy, policies and service levels.
- Ensure that automated business transactions and information exchanges can be trusted.
- Ensure that critical and confidential information is withheld from those who should not have access to it.
- Ensure minimum business impact in the event of an IT service disruption or change.
- Ensure proper use and performance of the applications and technology solutions.
- Ensure that IT services and infrastructure can properly resist and recover from failure due to error, delivered attack or disaster.

Process

- Develop a common and comprehensive IT control framework.
- Develop a common and comprehensive set of IT policies.
- Communicate the IT strategy, policies and control framework.

Activities

- Defining an IT control framework
- Developing and rolling out IT policies
- Enforcing IT policies
- Defining and maintaining a communications plan

Metrics

- Number of instances where confidential information was compromised
- Number of business disruptions due to IT service disruption
- Level of understanding of IT costs, benefits, strategy, policies and service levels

- Percent of stakeholders who understand IT policy
- Percent of stakeholders who understand the enterprise IT control framework
- Percent of stakeholders who are non-compliant with policy

- Frequency of policy review/update
- Timeliness and frequency of communication to users
- Frequency of enterprise IT control framework review/update

Maturity Model

PO6 Communicate Management Aims and Direction

Management of the process of *Communicate management aims and direction* that satisfies the business requirement for IT of *supplying accurate and timely information on current and future IT services and associated risks and responsibilities* is:

0 Non-existent when
Management has not established a positive IT control environment. There is no recognition of the need to establish a set of policies, plans and procedures, and compliance processes.

1 Initial/*Ad Hoc* when
Management is reactive in addressing the requirements of the information control environment. Policies, procedures and standards are developed and communicated on an *ad hoc* basis as driven by issues. The development, communication and compliance processes are informal and inconsistent.

2 Repeatable but Intuitive when
The needs and requirements of an effective information control environment are implicitly understood by management, but practices are largely informal. The need for control policies, plans and procedures is communicated by management, but development is left to the discretion of individual managers and business areas. Quality is recognised as a desirable philosophy to be followed, but practices are left to the discretion of individual managers. Training is carried out on an individual, as-required basis.

3 Defined when
A complete information control and quality management environment is developed, documented and communicated by management and includes a framework for policies, plans and procedures. The policy development process is structured, maintained and known to staff, and the existing policies, plans and procedures are reasonably sound and cover key issues. Management addresses the importance of IT security awareness and initiates awareness programmes. Formal training is available to support the information control environment but is not rigorously applied. Whilst there is an overall development framework for control policies and procedures, there is inconsistent monitoring of compliance with these policies and procedures. There is an overall development framework. Techniques for promoting security awareness have been standardised and formalised.

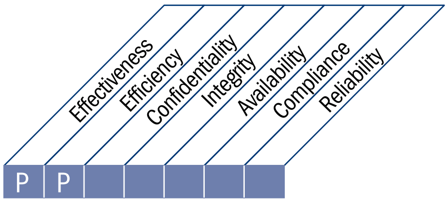
4 Managed and Measurable when
Management accepts responsibility for communicating internal control policies and delegates responsibility and allocates sufficient resources to maintain the environment in line with significant changes. A positive, proactive information control environment, including a commitment to quality and IT security awareness, is established. A complete set of policies, plans and procedures is developed, maintained and communicated and is a composite of internal good practices. A framework for rollout and subsequent compliance checks is established.

5 Optimised when
The information control environment is aligned with the strategic management framework and vision and is frequently reviewed, updated and continuously improved. Internal and external experts are assigned to ensure that industry good practices are being adopted with respect to control guidance and communication techniques. Monitoring, self-assessment and compliance checking are pervasive within the organisation. Technology is used to maintain policy and awareness knowledge bases and to optimise communication, using office automation and computer-based training tools.

Process Description

PO7 Manage IT Human Resources

A competent workforce is acquired and maintained for the creation and delivery of IT services to the business. This is achieved by following defined and agreed-upon practices supporting recruiting, training, evaluating performance, promoting and terminating. This process is critical, as people are important assets, and governance and the internal control environment are heavily dependent on the motivation and competence of personnel.



Control over the IT process of

Manage IT human resources

that satisfies the business requirement for IT of

acquiring competent and motivated people to create and deliver IT services

by focusing on

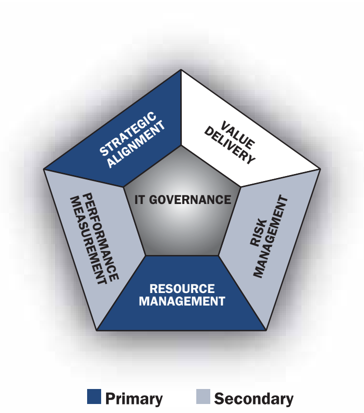
hiring and training personnel, motivating through clear career paths, assigning roles that correspond with skills, establishing a defined review process, creating position descriptions and ensuring awareness of dependency on individuals

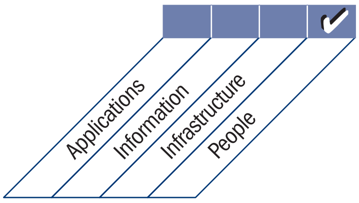
is achieved by

- Reviewing staff performance
- Hiring and training IT personnel to support IT tactical plans
- Mitigating the risk of overdependence on key resources

and is measured by

- Level of stakeholders' satisfaction with IT personnel expertise and skills
- IT personnel turnover
- Percent of IT personnel certified according to job needs





Control Objectives

PO7 Manage IT Human Resources

PO7.1 Personnel Recruitment and Retention

Maintain IT personnel recruitment processes in line with the overall organisation's personnel policies and procedures (e.g., hiring, positive work environment, orienting). Implement processes to ensure that the organisation has an appropriately deployed IT workforce with the skills necessary to achieve organisational goals.

PO7.2 Personnel Competencies

Regularly verify that personnel have the competencies to fulfil their roles on the basis of their education, training and/or experience. Define core IT competency requirements and verify that they are being maintained, using qualification and certification programmes where appropriate.

PO7.3 Staffing of Roles

Define, monitor and supervise roles, responsibilities and compensation frameworks for personnel, including the requirement to adhere to management policies and procedures, the code of ethics, and professional practices. The level of supervision should be in line with the sensitivity of the position and extent of responsibilities assigned.

PO7.4 Personnel Training

Provide IT employees with appropriate orientation when hired and ongoing training to maintain their knowledge, skills, abilities, internal controls and security awareness at the level required to achieve organisational goals.

PO7.5 Dependence Upon Individuals

Minimise the exposure to critical dependency on key individuals through knowledge capture (documentation), knowledge sharing, succession planning and staff backup.

PO7.6 Personnel Clearance Procedures

Include background checks in the IT recruitment process. The extent and frequency of periodic reviews of these checks should depend on the sensitivity and/or criticality of the function and should be applied for employees, contractors and vendors.

PO7.7 Employee Job Performance Evaluation

Require a timely evaluation to be performed on a regular basis against individual objectives derived from the organisation's goals, established standards and specific job responsibilities. Employees should receive coaching on performance and conduct whenever appropriate.

PO7.8 Job Change and Termination

Take expedient actions regarding job changes, especially job terminations. Knowledge transfer should be arranged, responsibilities reassigned and access rights removed such that risks are minimised and continuity of the function is guaranteed.

Management Guidelines

PO7 Manage IT Human Resources

From	Inputs
PO4	IT organisation and relationships; documented roles and responsibilities
AI1	Business requirements feasibility study

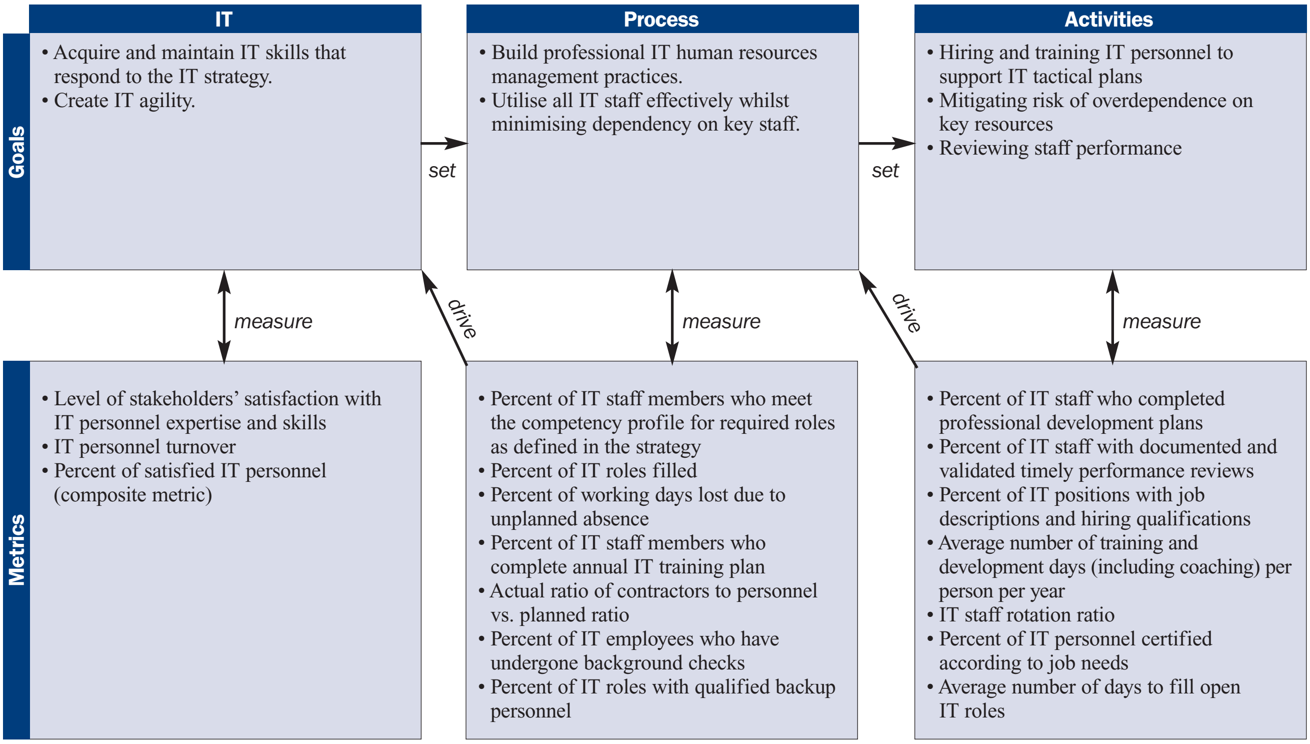
Outputs	To						
IT human resources policy and procedures	PO4						
IT skills matrix	PO4	PO10					
Job descriptions	PO4						
Users' skills and competencies, including individual training	DS7						
Specific training requirements	DS7						
Roles and responsibilities	ALL						

RACI Chart

Activities	CEO	CFO	Business Executive	CIO	Business Process Owner	Head Operations	Chief Architect	Head Development	Head IT Administration	PMO	Compliance, Audit, Risk and Security
Identify IT skills, position descriptions, salary ranges and personal performance benchmarks.		C		A		C	C	C	R	C	
Execute HR policies and procedures relevant to IT (recruit, hire, vet, compensate, train, appraise, promote and dismiss).				A		R	R	R	R	R	C

A **RACI** chart identifies who is **R**esponsible, **A**ccountable, **C**onsulted and/or **I**nformed.

Goals and Metrics



IT

Goals:
- Acquire and maintain IT skills that respond to the IT strategy.
- Create IT agility.

Metrics:
- Level of stakeholders' satisfaction with IT personnel expertise and skills
- IT personnel turnover
- Percent of satisfied IT personnel (composite metric)

Process

Goals:
- Build professional IT human resources management practices.
- Utilise all IT staff effectively whilst minimising dependency on key staff.

Metrics:
- Percent of IT staff members who meet the competency profile for required roles as defined in the strategy
- Percent of IT roles filled
- Percent of working days lost due to unplanned absence
- Percent of IT staff members who complete annual IT training plan
- Actual ratio of contractors to personnel vs. planned ratio
- Percent of IT employees who have undergone background checks
- Percent of IT roles with qualified backup personnel

Activities

Goals:
- Hiring and training IT personnel to support IT tactical plans
- Mitigating risk of overdependence on key resources
- Reviewing staff performance

Metrics:
- Percent of IT staff who completed professional development plans
- Percent of IT staff with documented and validated timely performance reviews
- Percent of IT positions with job descriptions and hiring qualifications
- Average number of training and development days (including coaching) per person per year
- IT staff rotation ratio
- Percent of IT personnel certified according to job needs
- Average number of days to fill open IT roles

Maturity Model

PO7 Manage IT Human Resources

Management of the process of *Manage IT human resources* that satisfies the business requirement for IT of *acquiring competent and motivated people to create and deliver IT services* is:

0 Non-existent when
There is no awareness about the importance of aligning IT human resources management with the technology planning process for the organisation. There is no person or group formally responsible for IT human resources management.

1 Initial/*Ad Hoc* when
Management recognises the need for IT human resources management. The IT human resources management process is informal and reactive. The IT human resources process is operationally focused on the hiring and managing of IT personnel. Awareness is developing concerning the impact that rapid business and technology changes and increasingly complex solutions have on the need for new skills and competence levels.

2 Repeatable but Intuitive when
There is a tactical approach to hiring and managing IT personnel, driven by project-specific needs, rather than by an understood balance of internal and external availability of skilled staff. Informal training takes place for new personnel, who then receive training on an as-required basis.

3 Defined when
There is a defined and documented process for managing IT human resources. An IT human resources management plan exists. There is a strategic approach to hiring and managing IT personnel. A formal training plan is designed to meet the needs of IT human resources. A rotational programme, designed to expand technical and business management skills, is established.

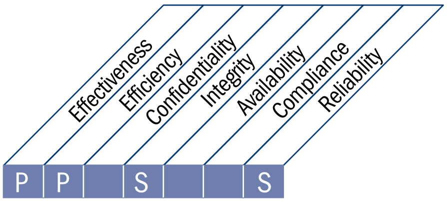
4 Managed and Measurable when
Responsibility for the development and maintenance of an IT human resources management plan is assigned to a specific individual or group with the requisite expertise and skills necessary to develop and maintain the plan. The process of developing and managing the IT human resources management plan is responsive to change. Standardised measures exist in the organisation to allow it to identify deviations from the IT human resources management plan, with specific emphasis on managing IT personnel growth and turnover. Compensation and performance reviews are being established and compared to other IT organisations and industry good practice. IT human resources management is proactive, taking into account career path development.

5 Optimised when
The IT human resources management plan is continuously being updated to meet changing business requirements. IT human resources management is integrated with technology planning, ensuring optimum development and use of available IT skills. IT human resources management is integrated with and responsive to the entity's strategic direction. Components of IT human resources management are consistent with industry good practices, such as compensation, performance reviews, participation in industry forums, transfer of knowledge, training and mentoring. Training programmes are developed for all new technology standards and products prior to their deployment in the organisation.

Process Description

PO8 Manage Quality

A QMS is developed and maintained that includes proven development and acquisition processes and standards. This is enabled by planning, implementing and maintaining the QMS by providing clear quality requirements, procedures and policies. Quality requirements are stated and communicated in quantifiable and achievable indicators. Continuous improvement is achieved by ongoing monitoring, analysis and acting upon deviations, and communicating results to stakeholders. Quality management is essential to ensure that IT is delivering value to the business, continuous improvement and transparency for stakeholders.



Plan and Organise
Acquire and Implement
Deliver and Support
Monitor and Evaluate

Control over the IT process of

Manage quality

that satisfies the business requirement for IT of

ensuring continuous and measurable improvement of the quality of IT services delivered

by focusing on

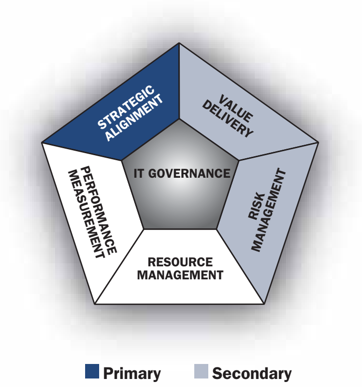
the definition of a QMS, ongoing performance monitoring against predefined objectives and implementation of a programme for continuous improvement of IT services

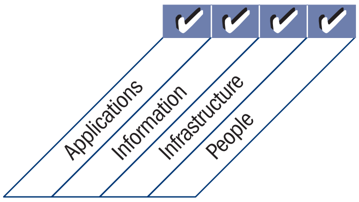
is achieved by

- Defining quality standards and practices
- Monitoring and reviewing internal and external performance against the defined quality standards and practices
- Improving the QMS in a continuous manner

and is measured by

- Percent of stakeholders satisfied with IT quality (weighted by importance)
- Percent of IT processes that are formally reviewed by QA on a periodic basis and that meet target quality goals and objectives
- Percent of processes receiving QA review





Control Objectives

PO8 Manage Quality

PO8.1 Quality Management System
Establish and maintain a QMS that provides a standard, formal and continuous approach regarding quality management that is aligned with business requirements. The QMS should identify quality requirements and criteria; key IT processes and their sequence and interaction; and the policies, criteria and methods for defining, detecting, correcting and preventing non-conformity. The QMS should define the organisational structure for quality management, covering the roles, tasks and responsibilities. All key areas should develop their quality plans in line with criteria and policies and record quality data. Monitor and measure the effectiveness and acceptance of the QMS, and improve it when needed

PO8.2 IT Standards and Quality Practices
Identify and maintain standards, procedures and practices for key IT processes to guide the organisation in meeting the intent of the QMS. Use industry good practices for reference when improving and tailoring the organisation's quality practices.

PO8.3 Development and Acquisition Standards
Adopt and maintain standards for all development and acquisition that follow the life cycle of the ultimate deliverable, and include sign-off at key milestones based on agreed-upon sign-off criteria. Consider software coding standards; naming conventions; file formats; schema and data dictionary design standards; user interface standards; interoperability; system performance efficiency; scalability; standards for development and testing; validation against requirements; test plans; and unit, regression and integration testing.

PO8.4 Customer Focus
Focus quality management on customers by determining their requirements and aligning them to the IT standards and practices. Define roles and responsibilities concerning conflict resolution between the user/customer and the IT organisation.

PO8.5 Continuous Improvement
Maintain and regularly communicate an overall quality plan that promotes continuous improvement.

PO8.6 Quality Measurement, Monitoring and Review
Define, plan and implement measurements to monitor continuing compliance to the QMS, as well as the value the QMS provides. Measurement, monitoring and recording of information should be used by the process owner to take appropriate corrective and preventive actions.

Management Guidelines

PO8 Manage Quality

From	Inputs
PO1	Strategic IT plan
PO10	Detailed project plans
ME1	Remedial action plans

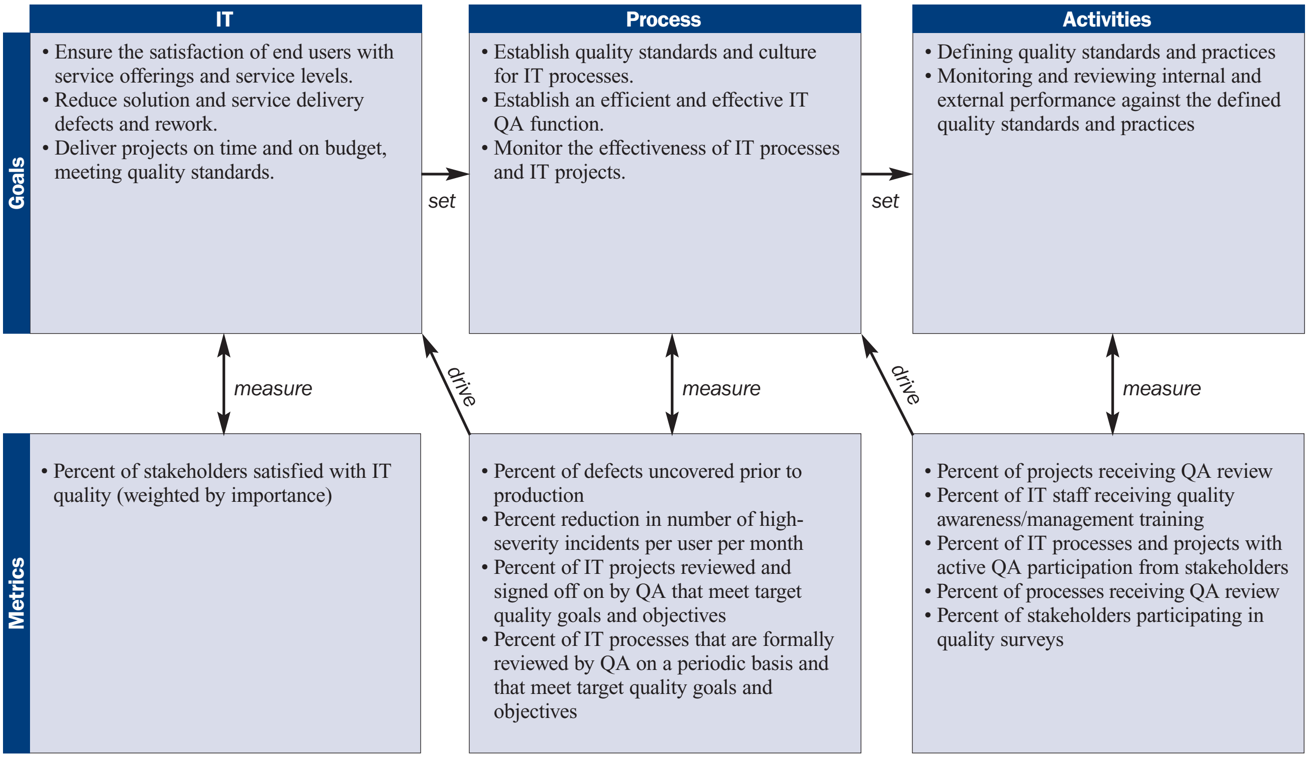
Outputs	To						
Acquisition standards	AI1	AI2	AI3	AI5	DS2		
Development standards	PO10	AI1	AI2	AI3	AI7		
Quality standards and metrics requirements	ALL						
Quality improvement actions	PO4	AI6					

RACI Chart

Activities \ Functions	CEO	CFO	Business Executive	CIO	Business Process Owner	Head Operations	Chief Architect	Head Development	Head IT Administration	PMO	Compliance, Audit, Risk and Security
Define a QMS.	C		C	A/R	I	I	I	I	I	I	C
Establish and maintain a QMS.	I	I	I	A/R	I	C	C	C	C	C	C
Build and communicate quality standards through the organisation.		I		A/R	I	C	C	C	C	C	C
Build and manage the quality plan for continuous improvement.				A/R	I	C	C	C	C	C	C
Measure, monitor and review compliance with the quality goals.				A/R	I	C	C	C	C	C	C

A **RACI** chart identifies who is **R**esponsible, **A**ccountable, **C**onsulted and/or **I**nformed.

Goals and Metrics



IT

Goals:
- Ensure the satisfaction of end users with service offerings and service levels.
- Reduce solution and service delivery defects and rework.
- Deliver projects on time and on budget, meeting quality standards.

Metrics:
- Percent of stakeholders satisfied with IT quality (weighted by importance)

Process

Goals:
- Establish quality standards and culture for IT processes.
- Establish an efficient and effective IT QA function.
- Monitor the effectiveness of IT processes and IT projects.

Metrics:
- Percent of defects uncovered prior to production
- Percent reduction in number of high-severity incidents per user per month
- Percent of IT projects reviewed and signed off on by QA that meet target quality goals and objectives
- Percent of IT processes that are formally reviewed by QA on a periodic basis and that meet target quality goals and objectives

Activities

Goals:
- Defining quality standards and practices
- Monitoring and reviewing internal and external performance against the defined quality standards and practices

Metrics:
- Percent of projects receiving QA review
- Percent of IT staff receiving quality awareness/management training
- Percent of IT processes and projects with active QA participation from stakeholders
- Percent of processes receiving QA review
- Percent of stakeholders participating in quality surveys

Maturity Model

PO8 Manage Quality

Management of the process of *Manage quality* that satisfies the business requirement for IT of *ensuring continuous and measurable improvement of the quality of IT services delivered* is:

0 Non-existent when
The organisation lacks a QMS planning process and a system development life cycle (SDLC) methodology. Senior management and IT staff members do not recognise that a quality programme is necessary. Projects and operations are never reviewed for quality.

1 Initial/*Ad Hoc* when
There is a management awareness of the need for a QMS. The QMS is driven by individuals where it takes place. Management makes informal judgements on quality.

2 Repeatable but Intuitive when
A programme is being established to define and monitor QMS activities within IT. QMS activities that do occur are focused on IT project- and process-oriented initiatives, not on organisationwide processes.

3 Defined when
A defined QMS process is communicated throughout the enterprise by management and involves IT and end-user management. An education and training programme is emerging to teach all levels of the organisation about quality. Basic quality expectations are defined and are shared amongst projects and within the IT organisation. Common tools and practices for quality management are emerging. Quality satisfaction surveys are planned and occasionally conducted.

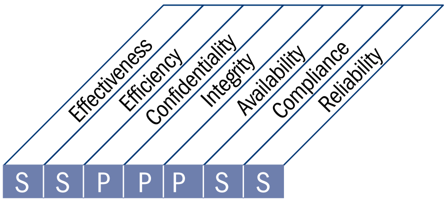
4 Managed and Measurable when
The QMS is addressed in all processes, including processes with reliance on third parties. A standardised knowledge base is being established for quality metrics. Cost-benefit analysis methods are used to justify QMS initiatives. Benchmarking against the industry and competitors is emerging. An education and training programme is instituted to teach all levels of the organisation about quality. Tools and practices are being standardised, and root cause analysis is periodically applied. Quality satisfaction surveys are consistently conducted. A standardised programme for measuring quality is in place and well structured. IT management is building a knowledge base for quality metrics.

5 Optimised when
The QMS is integrated and enforced in all IT activities. QMS processes are flexible and adaptable to changes in the IT environment. The knowledge base for quality metrics is enhanced with external good practices. Benchmarking against external standards is routinely performed. Quality satisfaction surveying is an ongoing process and leads to root cause analysis and improvement actions. There is formal assurance on the level of the quality management process.

Process Description

PO9 Assess and Manage IT Risks

A risk management framework is created and maintained. The framework documents a common and agreed-upon level of IT risks, mitigation strategies and residual risks. Any potential impact on the goals of the organisation caused by an unplanned event is identified, analysed and assessed. Risk mitigation strategies are adopted to minimise residual risk to an accepted level. The result of the assessment is understandable to the stakeholders and expressed in financial terms, to enable stakeholders to align risk to an acceptable level of tolerance.



Control over the IT process of

Assess and manage IT risks

that satisfies the business requirement for IT of

analysing and communicating IT risks and their potential impact on business processes and goals

by focusing on

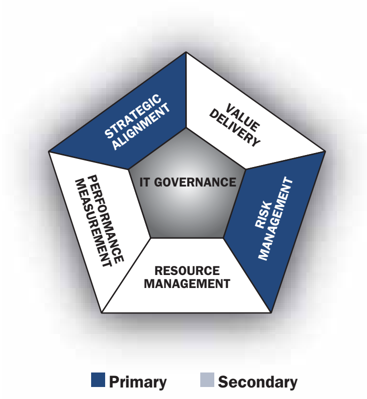
development of a risk management framework that is integrated in business and operational risk management frameworks, risk assessment, risk mitigation and communication of residual risk

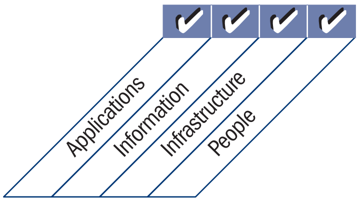
is achieved by

- Ensuring that risk management is fully embedded in management processes, internally and externally, and consistently applied
- Performing risk assessments
- Recommending and communicating risk remediation action plans

and is measured by

- Percent of critical IT objectives covered by risk assessment
- Percent of identified critical IT risks with action plans developed
- Percent of risk management action plans approved for implementation





Control Objectives

PO9 Assess and Manage IT Risks

PO9.1 IT Risk Management Framework
Establish an IT risk management framework that is aligned to the organisation's (enterprise's) risk management framework.

PO9.2 Establishment of Risk Context
Establish the context in which the risk assessment framework is applied to ensure appropriate outcomes. This should include determining the internal and external context of each risk assessment, the goal of the assessment, and the criteria against which risks are evaluated.

PO9.3 Event Identification
Identify events (an important realistic threat that exploits a significant applicable vulnerability) with a potential negative impact on the goals or operations of the enterprise, including business, regulatory, legal, technology, trading partner, human resources and operational aspects. Determine the nature of the impact and maintain this information. Record and maintain relevant risks in a risk registry.

PO9.4 Risk Assessment
Assess on a recurrent basis the likelihood and impact of all identified risks, using qualitative and quantitative methods. The likelihood and impact associated with inherent and residual risk should be determined individually, by category and on a portfolio basis.

PO9.5 Risk Response
Develop and maintain a risk response process designed to ensure that cost-effective controls mitigate exposure to risks on a continuing basis. The risk response process should identify risk strategies such as avoidance, reduction, sharing or acceptance; determine associated responsibilities; and consider risk tolerance levels.

PO9.6 Maintenance and Monitoring of a Risk Action Plan
Prioritise and plan the control activities at all levels to implement the risk responses identified as necessary, including identification of costs, benefits and responsibility for execution. Obtain approval for recommended actions and acceptance of any residual risks, and ensure that committed actions are owned by the affected process owner(s). Monitor execution of the plans, and report on any deviations to senior management.

Management Guidelines

PO9 Assess and Manage IT Risks

From	Inputs
PO1	Strategic and tactical IT plans, IT service portfolio
PO10	Project risk management plan
DS2	Supplier risks
DS4	Contingency test results
DS5	Security threats and vulnerabilities
ME1	Historical risk trends and events
ME4	Enterprise appetite for IT risks

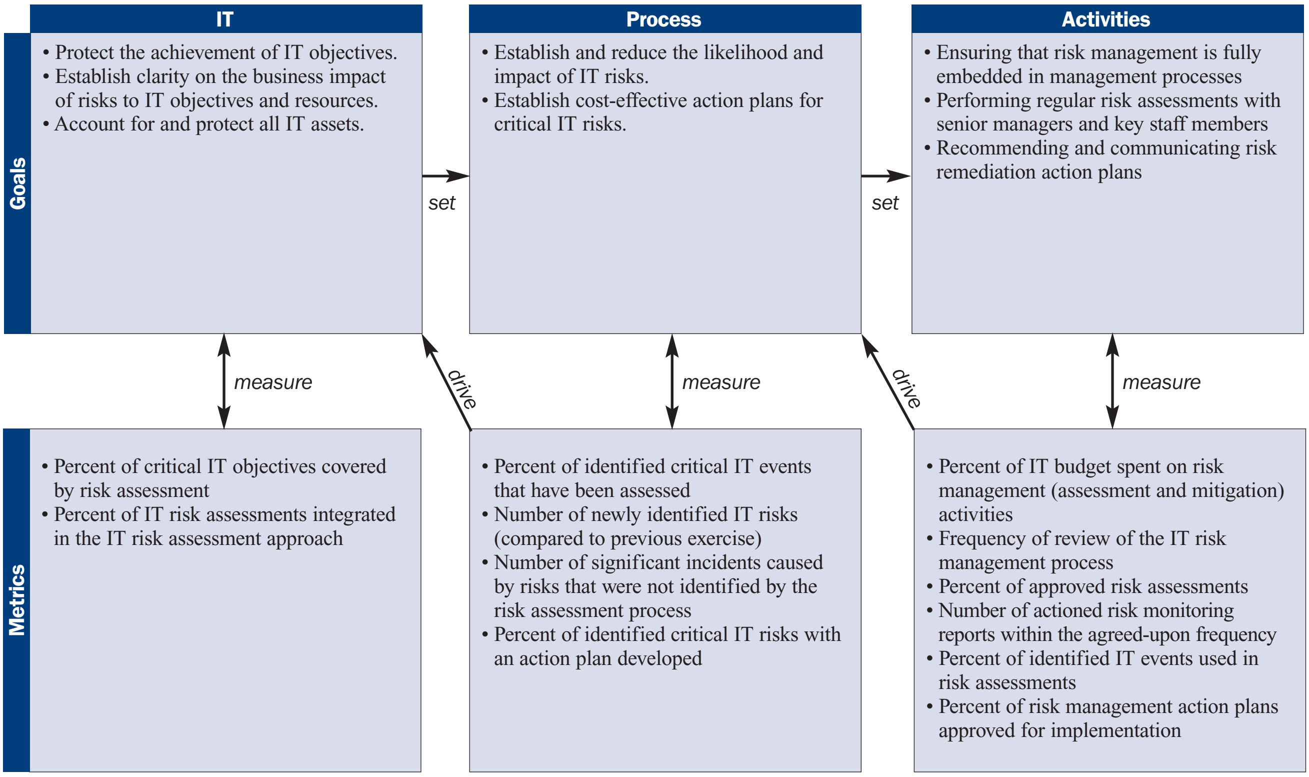
Outputs	To						
Risk assessment	PO1	DS4	DS5	DS12	ME4		
Risk reporting	ME4						
IT-related risk management guidelines	PO6						
IT-related risk remedial action plans	PO4	AI6					

RACI Chart

Activities	CEO	CFO	Business Executive	CIO	Business Senior Mangement	Head Operations	Chief Architect	Head Development	Head IT Administration	PMO	Compliance, Audit, Risk and Security
Determine risk management alignment (e.g., assess risk).	A	R/A	C	C	R/A	I					I
Understand relevant strategic business objectives.		C	C	R/A	C	C					I
Understand relevant business process objectives.				C	C	R/A					I
Identify internal IT objectives, and establish risk context.					R/A		C	C	C		I
Identify events associated with objectives (some events are business-oriented [business is A]; some are IT-oriented [IT is A, business is C]).	I			A/C	A	R	R	R	R		C
Assess risk associated with events.				A/C	A	R	R	R	R		C
Evaluate and select risk responses.	I	I	A	A/C	A	R	R	R	R		C
Prioritise and plan control activities.	C	C	A	A	R	R	C	C	C		C
Approve and ensure funding for risk action plans.		A	A		R	I	I	I	I		I
Maintain and monitor a risk action plan.	A	C	I	R	R	C	C	C	C	C	R

A **RACI** chart identifies who is **R**esponsible, **A**ccountable, **C**onsulted and/or **I**nformed.

Goals and Metrics



IT

Goals:
- Protect the achievement of IT objectives.
- Establish clarity on the business impact of risks to IT objectives and resources.
- Account for and protect all IT assets.

Metrics:
- Percent of critical IT objectives covered by risk assessment
- Percent of IT risk assessments integrated in the IT risk assessment approach

Process

Goals:
- Establish and reduce the likelihood and impact of IT risks.
- Establish cost-effective action plans for critical IT risks.

Metrics:
- Percent of identified critical IT events that have been assessed
- Number of newly identified IT risks (compared to previous exercise)
- Number of significant incidents caused by risks that were not identified by the risk assessment process
- Percent of identified critical IT risks with an action plan developed

Activities

Goals:
- Ensuring that risk management is fully embedded in management processes
- Performing regular risk assessments with senior managers and key staff members
- Recommending and communicating risk remediation action plans

Metrics:
- Percent of IT budget spent on risk management (assessment and mitigation) activities
- Frequency of review of the IT risk management process
- Percent of approved risk assessments
- Number of actioned risk monitoring reports within the agreed-upon frequency
- Percent of identified IT events used in risk assessments
- Percent of risk management action plans approved for implementation

Maturity Model

PO9 Assess and Manage IT Risks

Management of the process of *Assess and manage IT risks* that satisfies the business requirement for IT of *analysing and communicating IT risks and their potential impact on business processes and goals* is:

0 Non-existent when
Risk assessment for processes and business decisions does not occur. The organisation does not consider the business impacts associated with security vulnerabilities and development project uncertainties. Risk management is not identified as relevant to acquiring IT solutions and delivering IT services.

1 Initial/*Ad Hoc* when
IT risks are considered in an *ad hoc* manner. Informal assessments of project risk take place as determined by each project. Risk assessments are sometimes identified in a project plan but are rarely assigned to specific managers. Specific IT-related risks, such as security, availability and integrity, are occasionally considered on a project-by-project basis. IT-related risks affecting day-to-day operations are seldom discussed at management meetings. Where risks have been considered, mitigation is inconsistent. There is an emerging understanding that IT risks are important and need to be considered.

2 Repeatable but Intuitive when
A developing risk assessment approach exists and is implemented at the discretion of the project managers. The risk management is usually at a high level and is typically applied only to major projects or in response to problems. Risk mitigation processes are starting to be implemented where risks are identified.

3 Defined when
An organisationwide risk management policy defines when and how to conduct risk assessments. Risk management follows a defined process that is documented. Risk management training is available to all staff members. Decisions to follow the risk management process and receive training are left to the individual's discretion. The methodology for the assessment of risk is convincing and sound and ensures that key risks to the business are identified. A process to mitigate key risks is usually instituted once the risks are identified. Job descriptions consider risk management responsibilities.

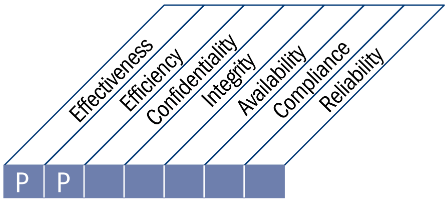
4 Managed and Measurable when
The assessment and management of risk are standard procedures. Exceptions to the risk management process are reported to IT management. IT risk management is a senior management-level responsibility. Risk is assessed and mitigated at the individual project level and also regularly with regard to the overall IT operation. Management is advised on changes in the business and IT environment that could significantly affect the IT-related risk scenarios. Management is able to monitor the risk position and make informed decisions regarding the exposure it is willing to accept. All identified risks have a nominated owner, and senior management and IT management determine the levels of risk that the organisation will tolerate. IT management develops standard measures for assessing risk and defining risk/return ratios. Management budgets for an operational risk management project to reassess risks on a regular basis. A risk management database is established, and part of the risk management processes is beginning to be automated. IT management considers risk mitigation strategies.

5 Optimised when
Risk management develops to the stage where a structured, organisationwide process is enforced and well managed. Good practices are applied across the entire organisation. The capture, analysis and reporting of risk management data are highly automated. Guidance is drawn from leaders in the field, and the IT organisation takes part in peer groups to exchange experiences. Risk management is truly integrated into all business and IT operations, is well accepted and extensively involves the users of IT services. Management detects and acts when major IT operational and investment decisions are made without consideration of the risk management plan. Management continually assesses risk mitigation strategies.

Process Description

PO10 Manage Projects

A programme and project management framework for the management of all IT projects is established. The framework ensures the correct prioritisation and co-ordination of all projects. The framework includes a master plan, assignment of resources, definition of deliverables, approval by users, a phased approach to delivery, QA, a formal test plan, and testing and post-implementation review after installation to ensure project risk management and value delivery to the business. This approach reduces the risk of unexpected costs and project cancellations, improves communications to and involvement of business and end users, ensures the value and quality of project deliverables, and maximises their contribution to IT-enabled investment programmes.



Control over the IT process of

Manage projects

that satisfies the business requirement for IT of

ensuring the delivery of project results within agreed-upon time frames, budget and quality

by focusing on

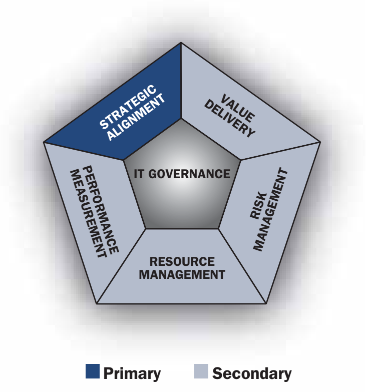
a defined programme and project management approach that is applied to IT projects and enables stakeholder participation in and monitoring of project risks and progress

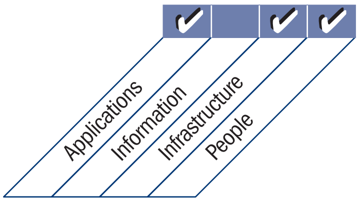
is achieved by

- Defining and enforcing programme and project frameworks and approach
- Issuing project management guidelines
- Performing project planning for each project detailed in the project portfolio

and is measured by

- Percent of projects meeting stakeholders' expectations (on time, on budget and meeting requirement—weighted by importance)
- Percent of projects receiving post-implementation reviews
- Percent of projects following project management standards and practices





Control Objectives

PO10 Manage Projects

PO10.1 Programme Management Framework
Maintain the programme of projects, related to the portfolio of IT-enabled investment programmes, by identifying, defining, evaluating, prioritising, selecting, initiating, managing and controlling projects. Ensure that the projects support the programme's objectives. Co-ordinate the activities and interdependencies of multiple projects, manage the contribution of all the projects within the programme to expected outcomes, and resolve resource requirements and conflicts.

PO10.2 Project Management Framework
Establish and maintain a project management framework that defines the scope and boundaries of managing projects, as well as the method to be adopted and applied to each project undertaken. The framework and supporting method should be integrated with the programme management processes.

PO10.3 Project Management Approach
Establish a project management approach commensurate with the size, complexity and regulatory requirements of each project. The project governance structure can include the roles, responsibilities and accountabilities of the programme sponsor, project sponsors, steering committee, project office and project manager, and the mechanisms through which they can meet those responsibilities (such as reporting and stage reviews). Make sure all IT projects have sponsors with sufficient authority to own the execution of the project within the overall strategic programme.

PO10.4 Stakeholder Commitment
Obtain commitment and participation from the affected stakeholders in the definition and execution of the project within the context of the overall IT-enabled investment programme.

PO10.5 Project Scope Statement
Define and document the nature and scope of the project to confirm and develop amongst stakeholders a common understanding of project scope and how it relates to other projects within the overall IT-enabled investment programme. The definition should be formally approved by the programme and project sponsors before project initiation.

PO10.6 Project Phase Initiation
Approve the initiation of each major project phase and communicate it to all stakeholders. Base the approval of the initial phase on programme governance decisions. Approval of subsequent phases should be based on review and acceptance of the deliverables of the previous phase, and approval of an updated business case at the next major review of the programme. In the event of overlapping project phases, an approval point should be established by programme and project sponsors to authorise project progression.

PO10.7 Integrated Project Plan
Establish a formal, approved integrated project plan (covering business and information systems resources) to guide project execution and control throughout the life of the project. The activities and interdependencies of multiple projects within a programme should be understood and documented. The project plan should be maintained throughout the life of the project. The project plan, and changes to it, should be approved in line with the programme and project governance framework.

PO10.8 Project Resources
Define the responsibilities, relationships, authorities and performance criteria of project team members, and specify the basis for acquiring and assigning competent staff members and/or contractors to the project. The procurement of products and services required for each project should be planned and managed to achieve project objectives using the organisation's procurement practices.

PO10.9 Project Risk Management
Eliminate or minimise specific risks associated with individual projects through a systematic process of planning, identifying, analysing, responding to, monitoring and controlling the areas or events that have the potential to cause unwanted change. Risks faced by the project management process and the project deliverable should be established and centrally recorded.

PO10.10 Project Quality Plan
Prepare a quality management plan that describes the project quality system and how it will be implemented. The plan should be formally reviewed and agreed to by all parties concerned and then incorporated into the integrated project plan.

PO10.11 Project Change Control
Establish a change control system for each project, so all changes to the project baseline (e.g., cost, schedule, scope, quality) are appropriately reviewed, approved and incorporated into the integrated project plan in line with the programme and project governance framework.

PO10.12 Project Planning of Assurance Methods
Identify assurance tasks required to support the accreditation of new or modified systems during project planning, and include them in the integrated project plan. The tasks should provide assurance that internal controls and security features meet the defined requirements.

PO10.13 Project Performance Measurement, Reporting and Monitoring
Measure project performance against key project performance scope, schedule, quality, cost and risk criteria. Identify any deviations from the plan. Assess the impact of deviations on the project and overall programme, and report results to key stakeholders. Recommend, implement and monitor remedial action, when required, in line with the programme and project governance framework.

PO10.14 Project Closure
Require that, at the end of each project, the project stakeholders ascertain whether the project delivered the planned results and benefits. Identify and communicate any outstanding activities required to achieve the planned results of the project and the benefits of the programme, and identify and document lessons learned for use on future projects and programmes.

Page intentionally left blank

Management Guidelines

PO10 Manage Projects

From	Inputs
PO1	IT project portfolio
PO5	Updated IT project portfolio
PO7	IT skills matrix
PO8	Development standards
AI7	Post-implementation review

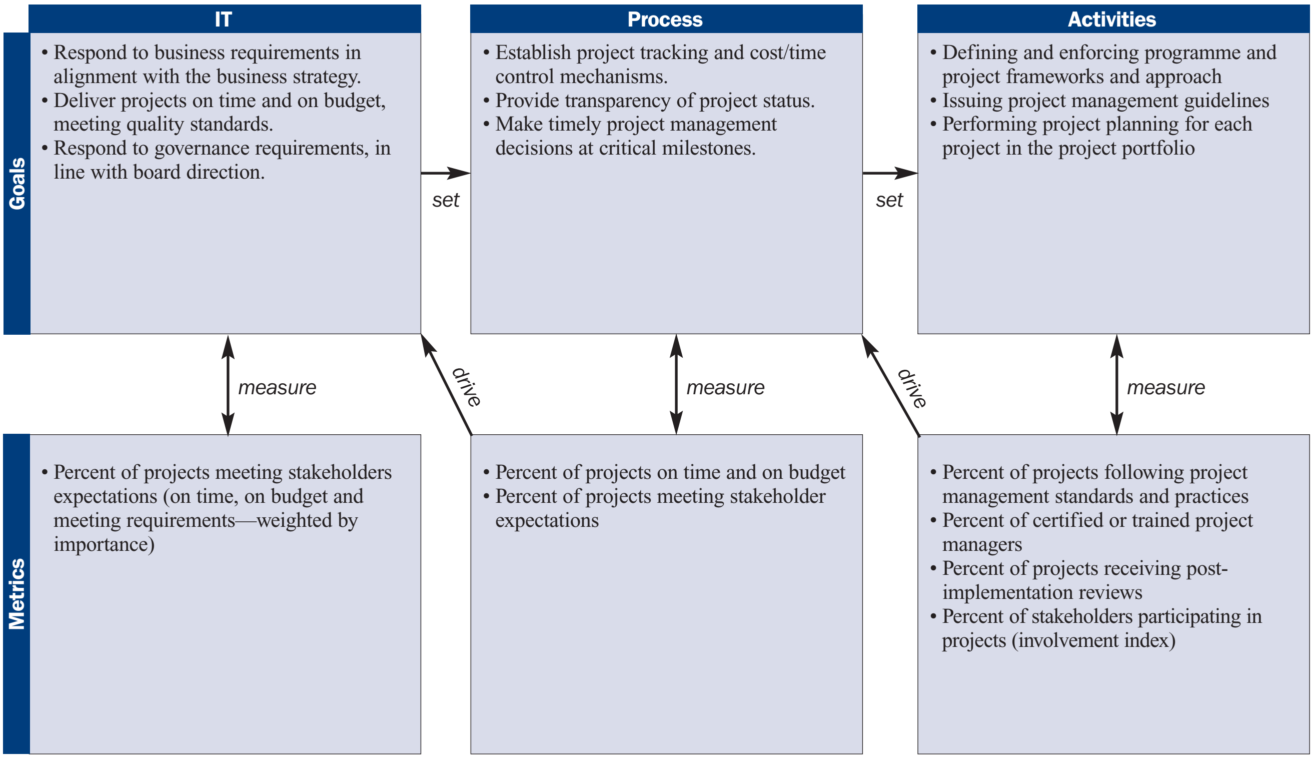
Outputs	To						
Project performance reports	ME1						
Project risk management plan	PO9						
Project management guidelines	AI1…AI7						
Detailed project plans	PO8	AI1…AI7		DS6			
Updated IT project portfolio	PO1	PO5					

RACI Chart

Activities \ Functions	CEO	CFO	Business Executive	CIO	Business Process Owner	Head Operations	Chief Architect	Head Development	Head IT Administration	PMO	Compliance, Audit, Risk and Security
Define a programme/portfolio management framework for IT investments.	C	C	A	R						C	C
Establish and maintain an IT project management framework.	I	I	I	A/R	I	C	C	C	C	R	C
Establish and maintain an IT project monitoring, measurement and management system.	I	I	I	R		C	C	C	C	A/R	C
Build project charters, schedules, quality plans, budgets, and communication and risk management plans.			C	C	C	C	C	C	C	A/R	C
Assure the participation and commitment of project stakeholders.	I		A	R	C						C
Assure the effective control of projects and project changes.			C	C		C	C	C		A/R	C
Define and implement project assurance and review methods.			I	C				I		A/R	C

A **RACI** charts identifies who is **R**esponsible, **A**ccountable, **C**onsulted and/or **I**nformed.

Goals and Metrics



Goals

IT
- Respond to business requirements in alignment with the business strategy.
- Deliver projects on time and on budget, meeting quality standards.
- Respond to governance requirements, in line with board direction.

Process
- Establish project tracking and cost/time control mechanisms.
- Provide transparency of project status.
- Make timely project management decisions at critical milestones.

Activities
- Defining and enforcing programme and project frameworks and approach
- Issuing project management guidelines
- Performing project planning for each project in the project portfolio

Metrics

- Percent of projects meeting stakeholders expectations (on time, on budget and meeting requirements—weighted by importance)

- Percent of projects on time and on budget
- Percent of projects meeting stakeholder expectations

- Percent of projects following project management standards and practices
- Percent of certified or trained project managers
- Percent of projects receiving post-implementation reviews
- Percent of stakeholders participating in projects (involvement index)

Maturity Model

PO10 Manage Projects

Management of the process of *Manage projects* that satisfies the business requirement for IT of *ensuring the delivery of project results within agreed-upon time frames, budget and quality* is:

0 Non-existent when
Project management techniques are not used and the organisation does not consider business impacts associated with project mismanagement and development project failures.

1 Initial/*Ad Hoc* when
The use of project management techniques and approaches within IT is a decision left to individual IT managers. There is a lack of management commitment to project ownership and project management. Critical decisions on project management are made without user management or customer input. There is little or no customer and user involvement in defining IT projects. There is no clear organisation within IT for the management of projects. Roles and responsibilities for the management of projects are not defined. Projects, schedules and milestones are poorly defined, if at all. Project staff time and expenses are not tracked and compared to budgets.

2 Repeatable but Intuitive when
Senior management gains and communicates an awareness of the need for IT project management. The organisation is in the process of developing and utilising some techniques and methods from project to project. IT projects have informally defined business and technical objectives. There is limited stakeholder involvement in IT project management. Initial guidelines are developed for many aspects of project management. Application of project management guidelines is left to the discretion of the individual project manager.

3 Defined when
The IT project management process and methodology are established and communicated. IT projects are defined with appropriate business and technical objectives. Senior IT and business management are beginning to be committed and involved in the management of IT projects. A project management office is established within IT, with initial roles and responsibilities defined. IT projects are monitored, with defined and updated milestones, schedules, budget and performance measurements. Project management training is available and is primarily a result of individual staff initiatives. QA procedures and post-system implementation activities are defined, but are not broadly applied by IT managers. Projects are beginning to be managed as portfolios.

4 Managed and Measurable when
Management requires formal and standardised project metrics and lessons learned to be reviewed following project completion. Project management is measured and evaluated throughout the organisation and not just within IT. Enhancements to the project management process are formalised and communicated with project team members trained on enhancements. IT management implements a project organisation structure with documented roles, responsibilities and staff performance criteria. Criteria for evaluating success at each milestone are established. Value and risk are measured and managed prior to, during and after the completion of projects. Projects increasingly address organisation goals, rather than only IT-specific ones. There is strong and active project support from senior management sponsors as well as stakeholders. Relevant project management training is planned for staff in the project management office and across the IT function.

5 Optimised when
A proven, full life cycle project and programme methodology is implemented, enforced and integrated into the culture of the entire organisation. An ongoing initiative to identify and institutionalise best project management practices is implemented. An IT strategy for sourcing development and operational projects is defined and implemented. An integrated project management office is responsible for projects and programmes from inception to post-implementation. Organisationwide planning of programmes and projects ensures that user and IT resources are best utilised to support strategic initiatives.

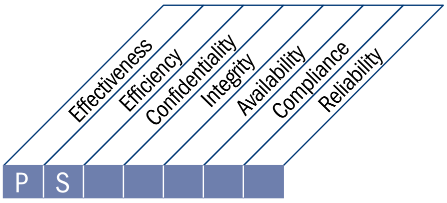
Acquire and Implement

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

Process Description

AI1 Identify Automated Solutions

The need for a new application or function requires analysis before acquisition or creation to ensure that business requirements are satisfied in an effective and efficient approach. This process covers the definition of the needs, consideration of alternative sources, review of technological and economic feasibility, execution of a risk analysis and cost-benefit analysis, and conclusion of a final decision to 'make' or 'buy'. All these steps enable organisations to minimise the cost to acquire and implement solutions whilst ensuring that they enable the business to achieve its objectives.



Control over the IT process of

Identify automated solutions

that satisfies the business requirement for IT of

translating business functional and control requirements into an effective and efficient design of automated solutions

by focusing on

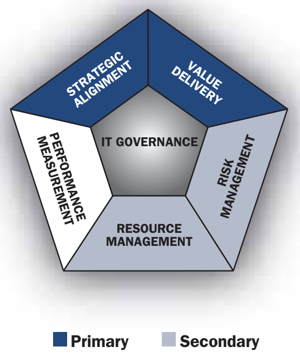
identifying technically feasible and cost-effective solutions

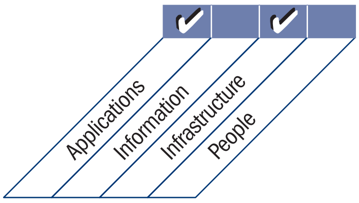
is achieved by

- Defining business and technical requirements
- Undertaking feasibility studies as defined in the development standards
- Approving (or rejecting) requirements and feasibility study results

and is measured by

- Number of projects where stated benefits were not achieved due to incorrect feasibility assumptions
- Percent of feasibility studies signed off on by the business process owner
- Percent of users satisfied with functionality delivered





CONTROL OBJECTIVES

AI1 Identify Automated Solutions

AI1.1 Definition and Maintenance of Business Functional and Technical Requirements
Identify, prioritise, specify and agree on business functional and technical requirements covering the full scope of all initiatives required to achieve the expected outcomes of the IT-enabled investment programme.

AI1.2 Risk Analysis Report
Identify, document and analyse risks associated with the business requirements and solution design as part of the organisation's process for the development of requirements.

AI1.3 Feasibility Study and Formulation of Alternative Courses of Action
Develop a feasibility study that examines the possibility of implementing the requirements. Business management, supported by the IT function, should assess the feasibility and alternative courses of action and make a recommendation to the business sponsor.

AI1.4 Requirements and Feasibility Decision and Approval
Verify that the process requires the business sponsor to approve and sign off on business functional and technical requirements and feasibility study reports at predetermined key stages. The business sponsor should make the final decision with respect to the choice of solution and acquisition approach.

Management Guidelines

AI1 Identify Automated Solutions

From	Inputs
PO1	Strategic and tactical IT plans
PO3	Regular ‘state of technology’ updates; technology standards
PO8	Acquisition and development standards
PO10	Project management guidelines and detailed project plans
AI6	Change process description
DS1	SLAs
DS3	Performance and capacity plan (requirements)

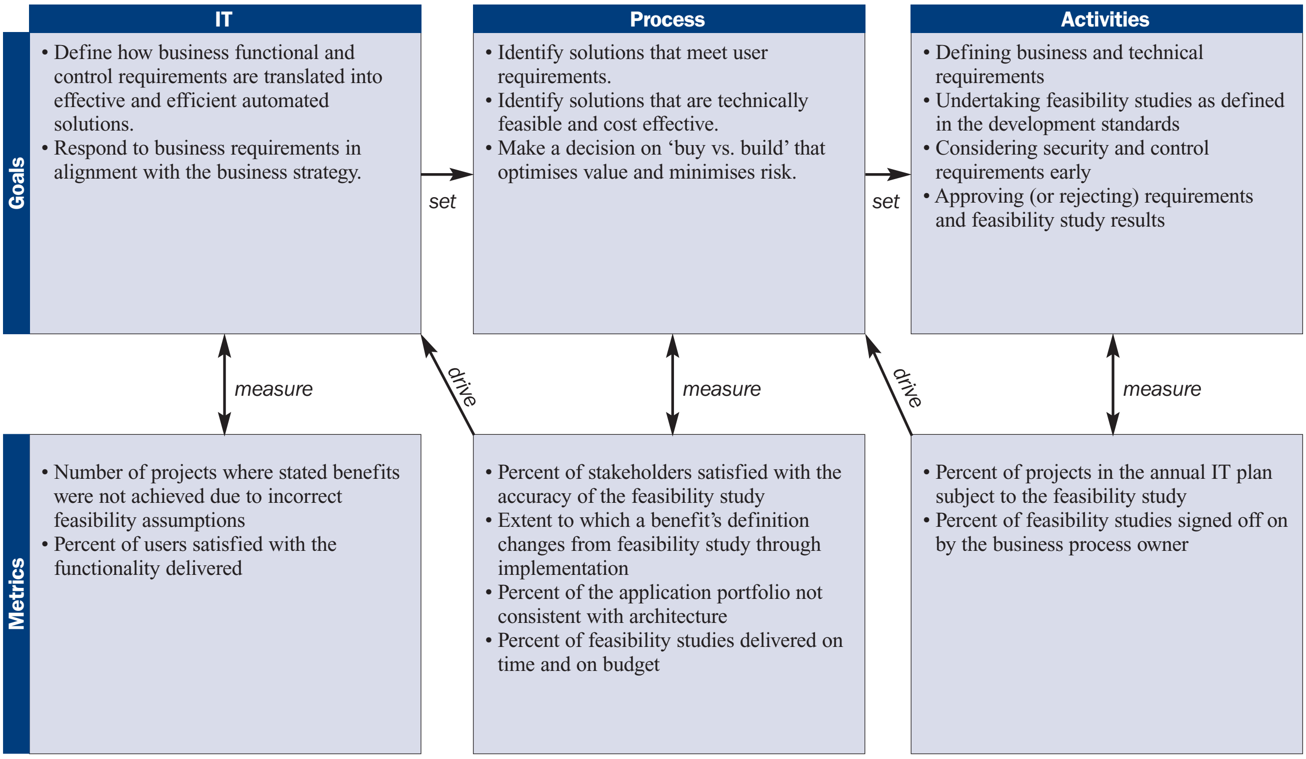
Outputs	To						
Business requirements feasibility study	PO2	PO5	PO7	AI2	AI3	AI4	AI5

RACI Chart

Activities \ Functions	CEO	CFO	Business Executive	CIO	Business Process Owner	Head Operations	Chief Architect	Head Development	Head IT Administration	PMO	Compliance, Audit, Risk and Security
Define business functional and technical requirements.			C	C	R	C	R	R		A/R	I
Establish processes for integrity/currency of requirements.				C		C		C		A/R	C
Identify, document and analyse business process risk.			A/R	R	R	R	C	R		R	C
Conduct a feasibility study/impact assessment in respect of implementing proposed business requirements.			A/R	R	R	C	C	C		R	C
Assess IT operational benefits of proposed solutions.		I	R	A/R	R	I	I	I		R	
Assess business benefits of proposed solutions.			A/R	R		C	C	C	I	R	
Develop a requirements approval process.			C	A		C	C	C		R	C
Approve and sign off on solutions proposed.		C	A/R	R	R	C	C	C	I	R	C

A **RACI** chart identifies who is **R**esponsible, **A**ccountable, **C**onsulted and/or **I**nformed.

Goals and Metrics



IT

Goals:
- Define how business functional and control requirements are translated into effective and efficient automated solutions.
- Respond to business requirements in alignment with the business strategy.

Metrics:
- Number of projects where stated benefits were not achieved due to incorrect feasibility assumptions
- Percent of users satisfied with the functionality delivered

Process

Goals:
- Identify solutions that meet user requirements.
- Identify solutions that are technically feasible and cost effective.
- Make a decision on ‘buy vs. build’ that optimises value and minimises risk.

Metrics:
- Percent of stakeholders satisfied with the accuracy of the feasibility study
- Extent to which a benefit’s definition changes from feasibility study through implementation
- Percent of the application portfolio not consistent with architecture
- Percent of feasibility studies delivered on time and on budget

Activities

Goals:
- Defining business and technical requirements
- Undertaking feasibility studies as defined in the development standards
- Considering security and control requirements early
- Approving (or rejecting) requirements and feasibility study results

Metrics:
- Percent of projects in the annual IT plan subject to the feasibility study
- Percent of feasibility studies signed off on by the business process owner

Maturity Model

AI1 Identify Automated Solutions

Management of the process of *Identify automated solutions* that satisfies the business requirement for IT of *translating business functional and control requirements into an effective and efficient design of automated solutions* is:

0 Non-existent when
The organisation does not require the identification of functional and operational requirements for development, implementation or modification of solutions, such as system, service, infrastructure, software and data. The organisation does not maintain an awareness of available technology solutions potentially relevant to its business.

1 Initial/*Ad Hoc* when
There is an awareness of the need to define requirements and identify technology solutions. Individual groups meet to discuss needs informally, and requirements are sometimes documented. Solutions are identified by individuals based on limited market awareness or in response to vendor offerings. There is minimal structured research or analysis of available technology.

2 Repeatable but Intuitive when
Some intuitive approaches to identify IT solutions exist and vary across the business. Solutions are identified informally based on the internal experience and knowledge of the IT function. The success of each project depends on the expertise of a few key individuals. The quality of documentation and decision making varies considerably. Unstructured approaches are used to define requirements and identify technology solutions.

3 Defined when
Clear and structured approaches in determining IT solutions exist. The approach to the determination of IT solutions requires the consideration of alternatives evaluated against business or user requirements, technological opportunities, economic feasibility, risk assessments, and other factors. The process for determining IT solutions is applied for some projects based on factors such as the decisions made by the individual staff members involved, the amount of management time committed, and the size and priority of the original business requirement. Structured approaches are used to define requirements and identify IT solutions.

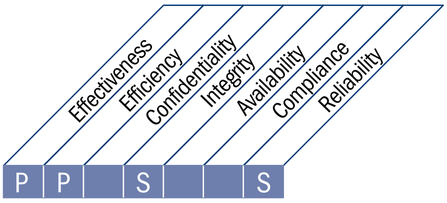
4 Managed and Measurable when
An established methodology for identification and assessment of IT solutions exists and is used for most projects. Project documentation is of good quality, and each stage is properly approved. Requirements are well articulated and in accordance with predefined structures. Solution alternatives are considered, including the analysis of costs and benefits. The methodology is clear, defined, generally understood and measurable. There is a clearly defined interface between IT management and business in the identification and assessment of IT solutions.

5 Optimised when
The methodology for identification and assessment of IT solutions is subjected to continuous improvement. The acquisition and implementation methodology has the flexibility for large- and small-scale projects. The methodology is supported by internal and external knowledge databases containing reference materials on technology solutions. The methodology itself produces documentation in a predefined structure that makes production and maintenance efficient. New opportunities are often identified to utilise technology to gain competitive advantage, influence business process re-engineering and improve overall efficiency. Management detects and acts if IT solutions are approved without consideration of alternative technologies or business functional requirements.

Process Description

AI2 Acquire and Maintain Application Software

Applications are made available in line with business requirements. This process covers the design of the applications, the proper inclusion of application controls and security requirements, and the development and configuration in line with standards. This allows organisations to properly support business operations with the correct automated applications.



Control over the IT process of

Acquire and maintain application software

that satisfies the business requirement for IT of

aligning available applications with business requirements, and doing so in a timely manner and at a reasonable cost

by focusing on

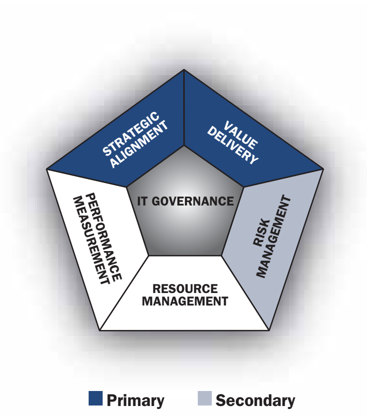
ensuring that there is a timely and cost-effective development process

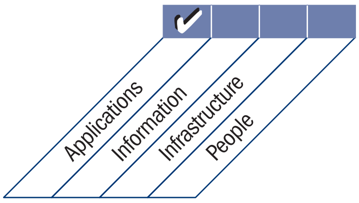
is achieved by

- Translating business requirements into design specifications
- Adhering to development standards for all modifications
- Separating development, testing and operational activities

and is measured by

- Number of production problems per application causing visible downtime
- Percent of users satisfied with the functionality delivered





Control Objectives

AI2 Acquire and Maintain Application Software

AI2.1 High-level Design
Translate business requirements into a high-level design specification for software acquisition, taking into account the organisation's technological direction and information architecture. Have the design specifications approved by management to ensure that the high-level design responds to the requirements. Reassess when significant technical or logical discrepancies occur during development or maintenance.

AI2.2 Detailed Design
Prepare detailed design and technical software application requirements. Define the criteria for acceptance of the requirements. Have the requirements approved to ensure that they correspond to the high-level design. Perform reassessment when significant technical or logical discrepancies occur during development or maintenance.

AI2.3 Application Control and Auditability
Implement business controls, where appropriate, into automated application controls such that processing is accurate, complete, timely, authorised and auditable.

AI2.4 Application Security and Availability
Address application security and availability requirements in response to identified risks and in line with the organisation's data classification, information architecture, information security architecture and risk tolerance.

AI2.5 Configuration and Implementation of Acquired Application Software
Configure and implement acquired application software to meet business objectives.

AI2.6 Major Upgrades to Existing Systems
In the event of major changes to existing systems that result in significant change in current designs and/or functionality, follow a similar development process as that used for the development of new systems.

AI2.7 Development of Application Software
Ensure that automated functionality is developed in accordance with design specifications, development and documentation standards, QA requirements, and approval standards. Ensure that all legal and contractual aspects are identified and addressed for application software developed by third parties.

AI2.8 Software Quality Assurance
Develop, resource and execute a software QA plan to obtain the quality specified in the requirements definition and the organisation's quality policies and procedures.

AI2.9 Applications Requirements Management
Track the status of individual requirements (including all rejected requirements) during the design, development and implementation, and approve changes to requirements through an established change management process.

AI2.10 Application Software Maintenance
Develop a strategy and plan for the maintenance of software applications.

Management Guidelines

AI2 Acquire and Maintain Application Software

From	Inputs
PO2	Data dictionary; data classification scheme; optimised business system plan
PO3	Regular 'state of technology' updates
PO5	Cost-benefits reports
PO8	Acquisition and development standards
PO10	Project management guidelines; detailed project plans
AI1	Business requirements feasibility study
AI6	Change process description

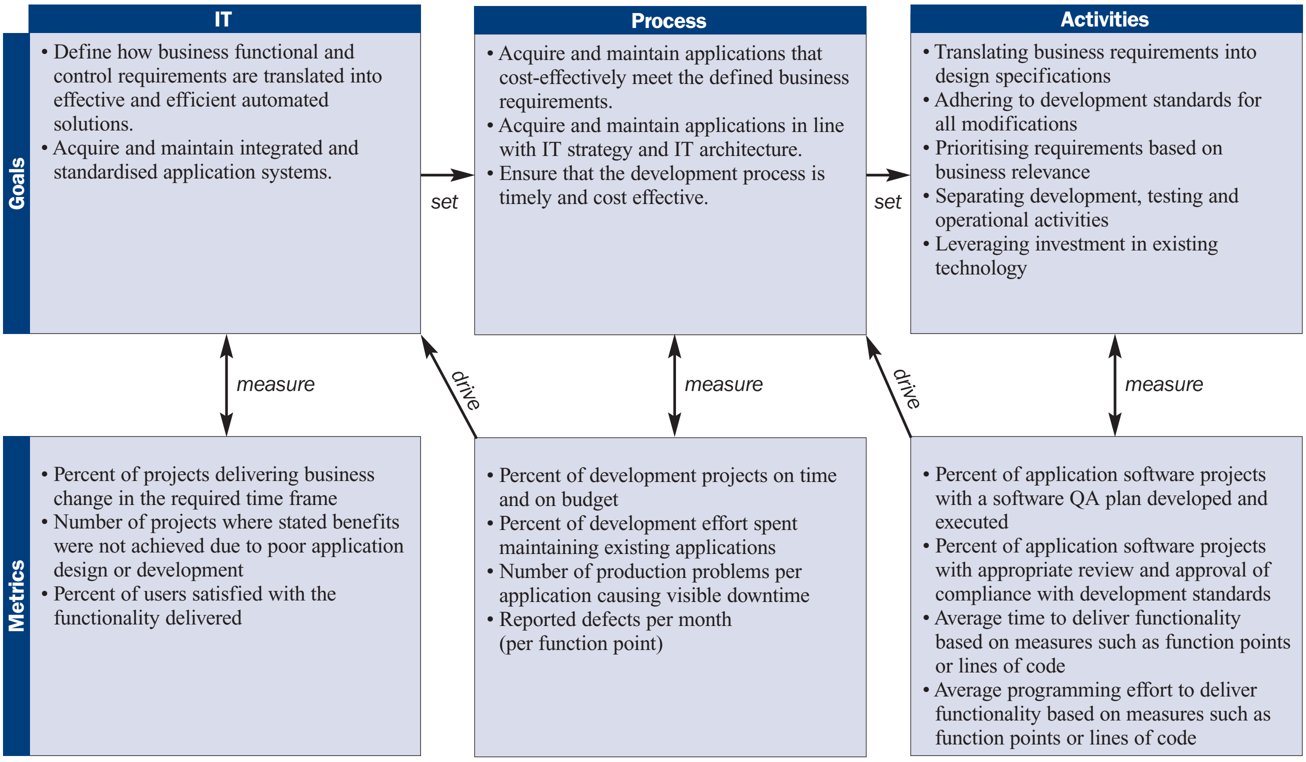
Outputs	To						
Application security controls specification	DS5						
Application and package software knowledge	AI4						
Procurement decisions	AI5						
Initial planned SLAs	DS1						
Availability, continuity and recovery specification	DS3	DS4					

RACI Chart

Activities / Functions	CEO	CFO	Business Executive	CIO	Business Process Owner	Head Operations	Chief Architect	Head Development	Head IT Administration	PMO	Compliance, Audit, Risk and Security
Translate business requirements into high-level design specifications.					C		C	A/R		R	C
Prepare detailed design and technical software application requirements.				I	C	C	C	A/R		R	C
Specify application controls within the design.					R	C		A/R		R	R
Customise and implement acquired automated functionality.					C	C		A/R		R	C
Develop formalised methodologies and processes to manage the application development process.				C		C	C	A	C	R	C
Create a software QA plan for the project.					I		C	R		A/R	C
Track and manage application requirements.								R		A/R	
Develop a plan for the maintenance of software applications.				C		C		A/R		C	

A **RACI** chart identifies who is **R**esponsible, **A**ccountable, **C**onsulted and/or **I**nformed.

Goals and Metrics



IT

Goals:
- Define how business functional and control requirements are translated into effective and efficient automated solutions.
- Acquire and maintain integrated and standardised application systems.

Metrics:
- Percent of projects delivering business change in the required time frame
- Number of projects where stated benefits were not achieved due to poor application design or development
- Percent of users satisfied with the functionality delivered

Process

Goals:
- Acquire and maintain applications that cost-effectively meet the defined business requirements.
- Acquire and maintain applications in line with IT strategy and IT architecture.
- Ensure that the development process is timely and cost effective.

Metrics:
- Percent of development projects on time and on budget
- Percent of development effort spent maintaining existing applications
- Number of production problems per application causing visible downtime
- Reported defects per month (per function point)

Activities

Goals:
- Translating business requirements into design specifications
- Adhering to development standards for all modifications
- Prioritising requirements based on business relevance
- Separating development, testing and operational activities
- Leveraging investment in existing technology

Metrics:
- Percent of application software projects with a software QA plan developed and executed
- Percent of application software projects with appropriate review and approval of compliance with development standards
- Average time to deliver functionality based on measures such as function points or lines of code
- Average programming effort to deliver functionality based on measures such as function points or lines of code

Maturity Model

AI2 Acquire and Maintain Application Software

Management of the process of *Acquire and maintain application software* that satisfies the business requirement for IT of *aligning available applications with business requirements, and doing so in a timely manner and at a reasonable cost* is:

0 Non-existent when
There is no process for designing and specifying applications. Typically, applications are obtained based on vendor-driven offerings, brand recognition or IT staff familiarity with specific products, with little or no consideration of actual requirements.

1 Initial/*Ad Hoc* when
There is an awareness that a process for acquiring and maintaining applications is required. Approaches to acquiring and maintaining application software vary from project to project. Some individual solutions to particular business requirements are likely to have been acquired independently, resulting in inefficiencies with maintenance and support.

2 Repeatable but Intuitive when
There are different, but similar, processes for acquiring and maintaining applications based on the expertise within the IT function. The success rate with applications depends greatly on the in-house skills and experience levels within IT. Maintenance is usually problematic and suffers when internal knowledge is lost from the organisation. There is little consideration of application security and availability in the design or acquisition of application software.

3 Defined when
A clear, defined and generally understood process exists for the acquisition and maintenance of application software. This process is aligned with IT and business strategy. An attempt is made to apply the documented processes consistently across different applications and projects. The methodologies are generally inflexible and difficult to apply in all cases, so steps are likely to be bypassed. Maintenance activities are planned, scheduled and co-ordinated.

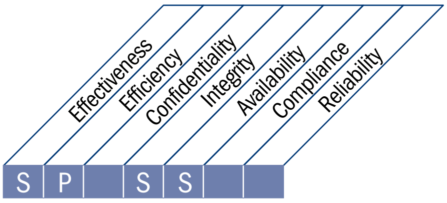
4 Managed and Measurable when
There is a formal and well-understood methodology that includes a design and specification process, criteria for acquisition, a process for testing and requirements for documentation. Documented and agreed-upon approval mechanisms exist to ensure that all steps are followed and exceptions are authorised. Practices and procedures evolve and are well suited to the organisation, used by all staff and applicable to most application requirements.

5 Optimised when
Application software acquisition and maintenance practices are aligned with the defined process. The approach is component-based, with predefined, standardised applications matched to business needs. The approach is enterprisewide. The acquisition and maintenance methodology is well advanced and enables rapid deployment, allowing for high responsiveness and flexibility in responding to changing business requirements. The application software acquisition and implementation methodology is subjected to continuous improvement and is supported by internal and external knowledge databases containing reference materials and good practices. The methodology creates documentation in a predefined structure that makes production and maintenance efficient.

Process Description

AI3 Acquire and Maintain Technology Infrastructure

Organisations have processes for the acquisition, implementation and upgrade of the technology infrastructure. This requires a planned approach to acquisition, maintenance and protection of infrastructure in line with agreed-upon technology strategies and the provision of development and test environments. This ensures that there is ongoing technological support for business applications.



Control over the IT process of

Acquire and maintain technology infrastructure

that satisfies the business requirement for IT of

acquiring and maintaining an integrated and standardised IT infrastructure

by focusing on

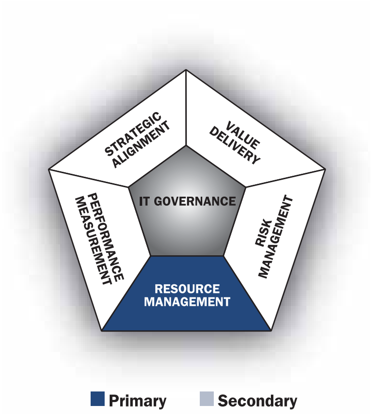
providing appropriate platforms for the business applications in line with the defined IT architecture and technology standards

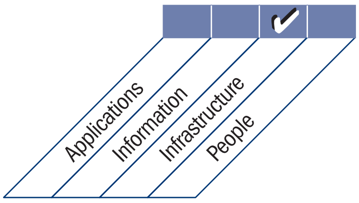
is achieved by

- Producing a technology acquisition plan that aligns to the technology infrastructure plan
- Planning infrastructure maintenance
- Implementing internal control, security and auditability measures

and is measured by

- Percent of platforms that are not in line with the defined IT architecture and technology standards
- Number of critical business processes supported by obsolete (or soon-to-be-obsolete) infrastructure
- Number of infrastructure components that are no longer supportable (or will not be in the near future)





Control Objectives

AI3 Acquire and Maintain Technology Infrastructure

AI3.1 Technological Infrastructure Acquisition Plan
Produce a plan for the acquisition, implementation and maintenance of the technological infrastructure that meets established business functional and technical requirements and is in accord with the organisation's technology direction.

AI3.2 Infrastructure Resource Protection and Availability
Implement internal control, security and auditability measures during configuration, integration and maintenance of hardware and infrastructural software to protect resources and ensure availability and integrity. Responsibilities for using sensitive infrastructure components should be clearly defined and understood by those who develop and integrate infrastructure components. Their use should be monitored and evaluated.

AI3.3 Infrastructure Maintenance
Develop a strategy and plan for infrastructure maintenance, and ensure that changes are controlled in line with the organisation's change management procedure. Include periodic reviews against business needs, patch management, upgrade strategies, risks, vulnerabilities assessment and security requirements.

AI3.4 Feasibility Test Environment
Establish development and test environments to support effective and efficient feasibility and integration testing of infrastructure components.

Management Guidelines

AI3 Acquire and Maintain Technology Infrastructure

From	Inputs
PO3	Technology infrastructure plan, standards and opportunitites; regular 'state of technology' updates
PO8	Acquisition and development standards
PO10	Project management guidelines and detailed project plans
AI1	Business requirements feasibility study
AI6	Change process description
DS3	Performance and capacity plan (requirements)

Outputs	To						
Procurement decisions	AI5						
Configured system to be tested/installed	AI7						
Physical environment requirements	DS12						
Updates for technology standards	PO3						
System monitoring requirements	DS3						
Infrastructure knowledge	AI4						
Initial planned operating level agreements (OLAs)	DS1						

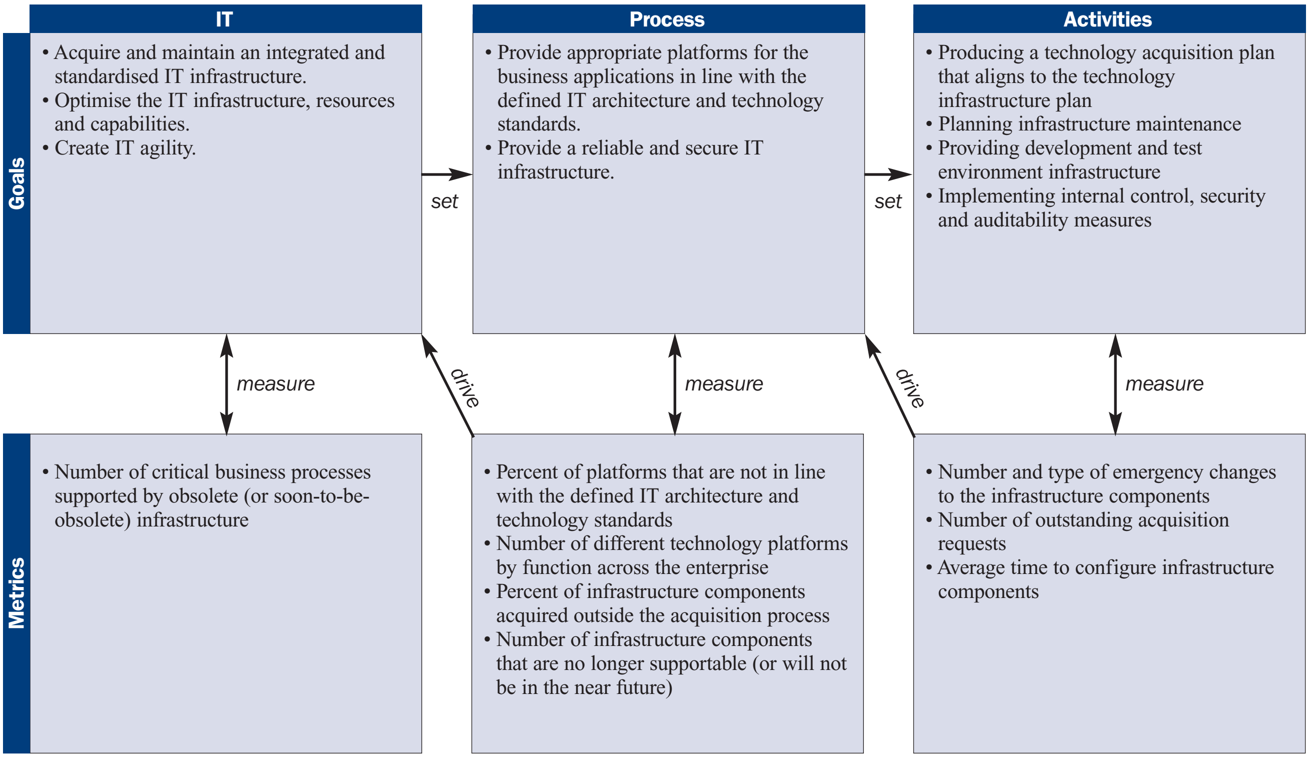
RACI Chart

Functions

Activities	CEO	CFO	Business Executive	CIO	Business Process Owner	Head Operations	Chief Architect	Head Development	Head IT Administration	PMO	Compliance, Audit, Risk and Security
Define the acquisition procedure/process.		C		A		C	C	C	R		I
Discuss infrastructure requirements with (approved) vendors.		C/I		A	I	R	C	C	R		I
Define strategy and plan maintenance for infrastructure.				A		R	R	R	C		
Configure the infrastructure components.				A		R	C				I

A **RACI** chart identifies who is **R**esponsible, **A**ccountable, **C**onsulted and/or **I**nformed.

Goals and Metrics



IT – Goals
- Acquire and maintain an integrated and standardised IT infrastructure.
- Optimise the IT infrastructure, resources and capabilities.
- Create IT agility.

Process – Goals
- Provide appropriate platforms for the business applications in line with the defined IT architecture and technology standards.
- Provide a reliable and secure IT infrastructure.

Activities – Goals
- Producing a technology acquisition plan that aligns to the technology infrastructure plan
- Planning infrastructure maintenance
- Providing development and test environment infrastructure
- Implementing internal control, security and auditability measures

IT – Metrics
- Number of critical business processes supported by obsolete (or soon-to-be-obsolete) infrastructure

Process – Metrics
- Percent of platforms that are not in line with the defined IT architecture and technology standards
- Number of different technology platforms by function across the enterprise
- Percent of infrastructure components acquired outside the acquisition process
- Number of infrastructure components that are no longer supportable (or will not be in the near future)

Activities – Metrics
- Number and type of emergency changes to the infrastructure components
- Number of outstanding acquisition requests
- Average time to configure infrastructure components

Maturity Model

AI3 Acquire and Maintain Technology Infrastructure

Management of the process of *Acquire and maintain technology infrastructure* that satisfies the business requirement for IT of *acquiring and maintaining an integrated and standardised IT infrastructure* is:

0 Non-existent when
Managing the technology infrastructure is not recognised as a sufficiently important topic to be addressed.

1 Initial/*Ad Hoc* when
There are changes made to infrastructure for every new application, without any overall plan. Although there is an awareness that the IT infrastructure is important, there is no consistent overall approach. Maintenance activity reacts to short-term needs. The production environment is the test environment.

2 Repeatable but Intuitive when
There is a consistency amongst tactical approaches when acquiring and maintaining the IT infrastructure. Acquisition and maintenance of IT infrastructure are not based on any defined strategy and do not consider the needs of the business applications that must be supported. There is an understanding that the IT infrastructure is important, supported by some formal practices. Some maintenance is scheduled, but it is not fully scheduled and co-ordinated. For some environments, a separate test environment exists.

3 Defined when
A clear, defined and generally understood process exists for acquiring and maintaining IT infrastructure. The process supports the needs of critical business applications and is aligned to IT and business strategy, but it is not consistently applied. Maintenance is planned, scheduled and co-ordinated. There are separate environments for test and production.

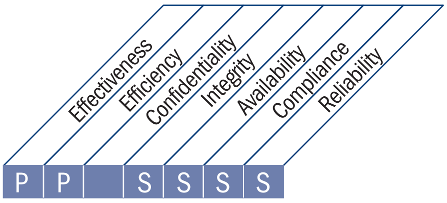
4 Managed and Measurable when
The acquisition and maintenance process for technology infrastructure has developed to the point where it works well for most situations, is followed consistently and is focused on reusability. The IT infrastructure adequately supports the business applications. The process is well organised and proactive. The cost and lead time to achieve the expected level of scalability, flexibility and integration are partially optimised.

5 Optimised when
The acquisition and maintenance process for technology infrastructure is proactive and closely aligned with critical business applications and the technology architecture. Good practices regarding technology solutions are followed, and the organisation is aware of the latest platform developments and management tools. Costs are reduced by rationalising and standardising infrastructure components and by using automation. A high level of technical awareness can identify optimum ways to proactively improve performance, including consideration of outsourcing options. The IT infrastructure is seen as the key enabler to leveraging the use of IT.

Process Description

AI4 Enable Operation and Use

Knowledge about new systems is made available. This process requires the production of documentation and manuals for users and IT, and provides training to ensure the proper use and operation of applications and infrastructure.



Control over the IT process of

Enable operation and use

that satisfies the business requirement for IT of

ensuring satisfaction of end users with service offerings and service levels and seamlessly integrating applications and technology solutions into business processes

by focusing on

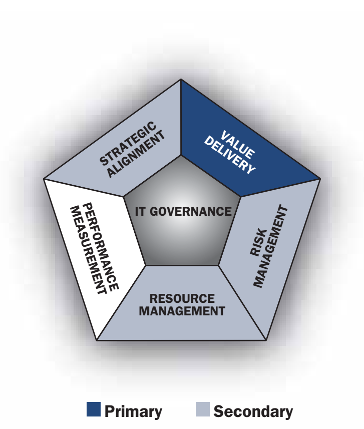
providing effective user and operational manuals and training materials to transfer the knowledge necessary for successful system operation and use

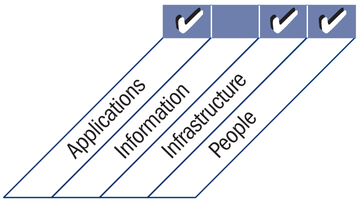
is achieved by

- Developing and making available knowledge transfer documentation
- Communicating and training users, business management, support staff and operational staff
- Producing training materials

and is measured by

- Number of applications where IT procedures are seamlessly integrated into business processes
- Percent of business owners satisfied with application training and support materials
- Number of applications with adequate user and operational support training





Control Objectives

AI4 Enable Operation and Use

AI4.1 Planning for Operational Solutions
Develop a plan to identify and document all technical, operational and usage aspects such that all those who will operate, use and maintain the automated solutions can exercise their responsibility.

AI4.2 Knowledge Transfer to Business Management
Transfer knowledge to business management to allow those individuals to take ownership of the system and data, and exercise responsibility for service delivery and quality, internal control, and application administration.

AI4.3 Knowledge Transfer to End Users
Transfer knowledge and skills to allow end users to effectively and efficiently use the system in support of business processes.

AI4.4 Knowledge Transfer to Operations and Support Staff
Transfer knowledge and skills to enable operations and technical support staff to effectively and efficiently deliver, support and maintain the system and associated infrastructure.

Management Guidelines

AI4 Enable Operation and Use

From	Inputs
PO10	Project management guidelines and detailed project plans
AI1	Business requirement feasibility study
AI2	Application and package software knowledge
AI3	Infrastructure knowledge
AI7	Known and accepted errors
DS7	Required documentation updates

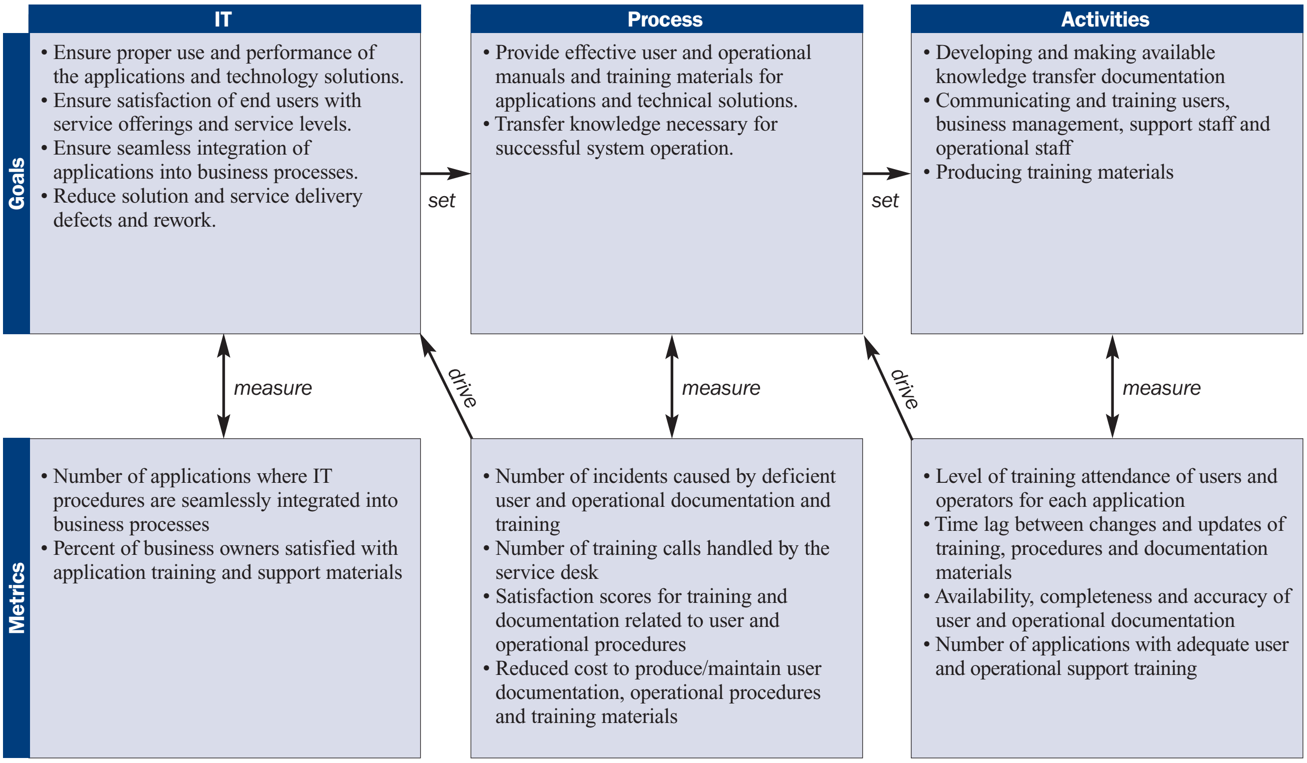
Outputs	To						
User, operational, support, technical and administration manuals	AI7	DS4	DS8	DS9	DS11	DS13	
Knowledge transfer requirements for a solution's implementation	DS7						
Training materials	DS7						

RACI Chart

Activities	CEO	CFO	Business Executive	CIO	Business Process Owner	Head Operations	Chief Architect	Head Development	Head IT Administration	PMO	Compliance, Audit, Risk and Security	Deployment Team	Training Department
Develop a strategy to operationalise the solution.				A	A	R		R			I	R	C
Develop a knowledge transfer methodology.				C	A							C	R
Develop end-user procedure manuals.					A/R			R			C	C	
Develop technical support documentation for operations and support staff.						A/R		C			C		
Develop and deliver training.					A	A		R					R
Evaluate training results and enhance documentation as required.					A	A						R	R

A **RACI** chart identifies who is **R**esponsible, **A**ccountable, **C**onsulted and/or **I**nformed.

Goals and Metrics



IT — Goals
- Ensure proper use and performance of the applications and technology solutions.
- Ensure satisfaction of end users with service offerings and service levels.
- Ensure seamless integration of applications into business processes.
- Reduce solution and service delivery defects and rework.

Process — Goals
- Provide effective user and operational manuals and training materials for applications and technical solutions.
- Transfer knowledge necessary for successful system operation.

Activities — Goals
- Developing and making available knowledge transfer documentation
- Communicating and training users, business management, support staff and operational staff
- Producing training materials

IT — Metrics
- Number of applications where IT procedures are seamlessly integrated into business processes
- Percent of business owners satisfied with application training and support materials

Process — Metrics
- Number of incidents caused by deficient user and operational documentation and training
- Number of training calls handled by the service desk
- Satisfaction scores for training and documentation related to user and operational procedures
- Reduced cost to produce/maintain user documentation, operational procedures and training materials

Activities — Metrics
- Level of training attendance of users and operators for each application
- Time lag between changes and updates of training, procedures and documentation materials
- Availability, completeness and accuracy of user and operational documentation
- Number of applications with adequate user and operational support training

Maturity Model

AI4 Enable Operation and Use

Management of the process of *Enable operation and use* that satisfies the business requirement for IT of *ensuring satisfaction of end users with service offerings and service levels and seamlessly integrating applications and technology solutions into business processes* is:

0 Non-existent when
There is no process in place with regard to the production of user documentation, operations manuals and training material. The only materials that exist are those supplied with purchased products.

1 Initial/*Ad Hoc* when
There is awareness that process documentation is needed. Documentation is occasionally produced and is inconsistently distributed to limited groups. Much of the documentation and many of the procedures are out of date. Training materials tend to be one-off schemes with variable quality. There is virtually no integration of procedures across different systems and business units. There is no input from business units in the design of training programmes.

2 Repeatable but Intuitive when
Similar approaches are used to produce procedures and documentation, but they are not based on a structured approach or framework. There is no uniform approach to the development of user and operating procedures. Training materials are produced by individuals or project teams, and quality depends on the individuals involved. Procedures and quality of user support vary from poor to very good, with very little consistency and integration across the organisation. Training programmes for the business and users are provided or facilitated, but there is no overall plan for training rollout or delivery.

3 Defined when
There is a clearly defined, accepted and understood framework for user documentation, operations manuals and training materials. Procedures are stored and maintained in a formal library and can be accessed by anyone who needs to know them. Corrections to documentation and procedures are made on a reactive basis. Procedures are available offline and can be accessed and maintained in case of disaster. A process exists that specifies procedure updates and training materials to be an explicit deliverable of a change project. Despite the existence of defined approaches, the actual content varies because there is no control to enforce compliance with standards. Users are informally involved in the process. Automated tools are increasingly used in the generation and distribution of procedures. Business and user training is planned and scheduled.

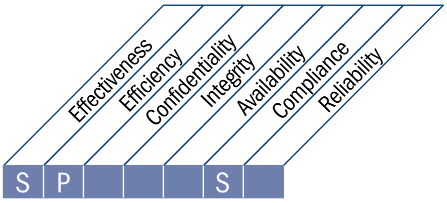
4 Managed and Measurable when
There is a defined framework for maintaining procedures and training materials that has IT management support. The approach taken for maintaining procedures and training manuals covers all systems and business units, so that processes can be viewed from a business perspective. Procedures and training materials are integrated to include interdependencies and interfaces. Controls exist to ensure adherence to standards, and procedures are developed and maintained for all processes. Business and user feedback on documentation and training is collected and assessed as part of a continuous improvement process. Documentation and training materials are usually at a predictable and good level of reliability and availability. An emerging process for using automated procedure documentation and management is implemented. Automated procedure development is increasingly integrated with application system development facilitating consistency and user access. Business and user training is responsive to the needs of the business. IT management is developing metrics for the development and delivery of documentation, training materials and training programmes.

5 Optimised when
The process for user and operational documentation is constantly improved through the adoption of new tools or methods. The procedure materials and training materials are treated as a constantly evolving knowledge base that is maintained electronically using up-to-date knowledge management, workflow and distribution technologies, making it accessible and easy to maintain. Documentation and training material is updated to reflect organisational, operational and software changes. The development of documentation and training materials and the delivery of training programmes are fully integrated with the business and business process definitions, thus supporting organisationwide requirements, rather than only IT-oriented procedures.

Process Description

AI5 Procure IT Resources

IT resources, including people, hardware, software and services, need to be procured. This requires the definition and enforcement of procurement procedures, the selection of vendors, the setup of contractual arrangements, and the acquisition itself. Doing so ensures that the organisation has all required IT resources in a timely and cost-effective manner.



Control over the IT process of

Procure IT resources

that satisfies the business requirement for IT of

improving IT's cost-efficiency and its contribution to business profitability

by focusing on

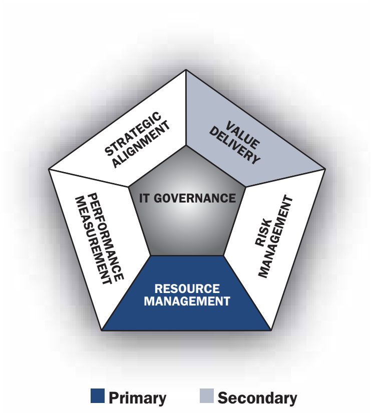
acquiring and maintaining IT skills that respond to the delivery strategy, an integrated and standardised IT infrastructure, and reducing IT procurement risk

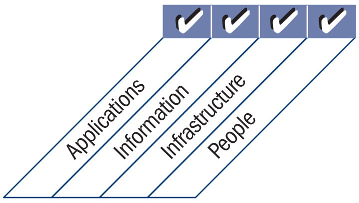
is achieved by

- Obtaining professional legal and contractual advice
- Defining procurement procedures and standards
- Procuring requested hardware, software and services in line with defined procedures

and is measured by

- Number of disputes related to procurement contracts
- Amount of reduction of the purchasing cost
- Percent of key stakeholders satisfied with suppliers





Control Objectives

AI5 Procure IT Resources

AI5.1 Procurement Control
Develop and follow a set of procedures and standards that is consistent with the business organisation's overall procurement process and acquisition strategy to acquire IT-related infrastructure, facilities, hardware, software and services needed by the business.

AI5.2 Supplier Contract Management
Set up a procedure for establishing, modifying and terminating contracts for all suppliers. The procedure should cover, at a minimum, legal, financial, organisational, documentary, performance, security, intellectual property, and termination responsibilities and liabilities (including penalty clauses). All contracts and contract changes should be reviewed by legal advisors.

AI5.3 Supplier Selection
Select suppliers according to a fair and formal practice to ensure a viable best fit based on specified requirements. Requirements should be optimised with input from potential suppliers.

AI5.4 IT Resources Acquisition
Protect and enforce the organisation's interests in all acquisition contractual agreements, including the rights and obligations of all parties in the contractual terms for the acquisition of software, development resources, infrastructure and services.

Management Guidelines

AI5 Procure IT Resources

From	Inputs
PO1	IT acquisition strategy
PO8	Acquisition standards
PO10	Project management guidelines and detailed project plans
AI1	Business requirement feasibility study
AI2-3	Procurement decisions
DS2	Supplier catalogue

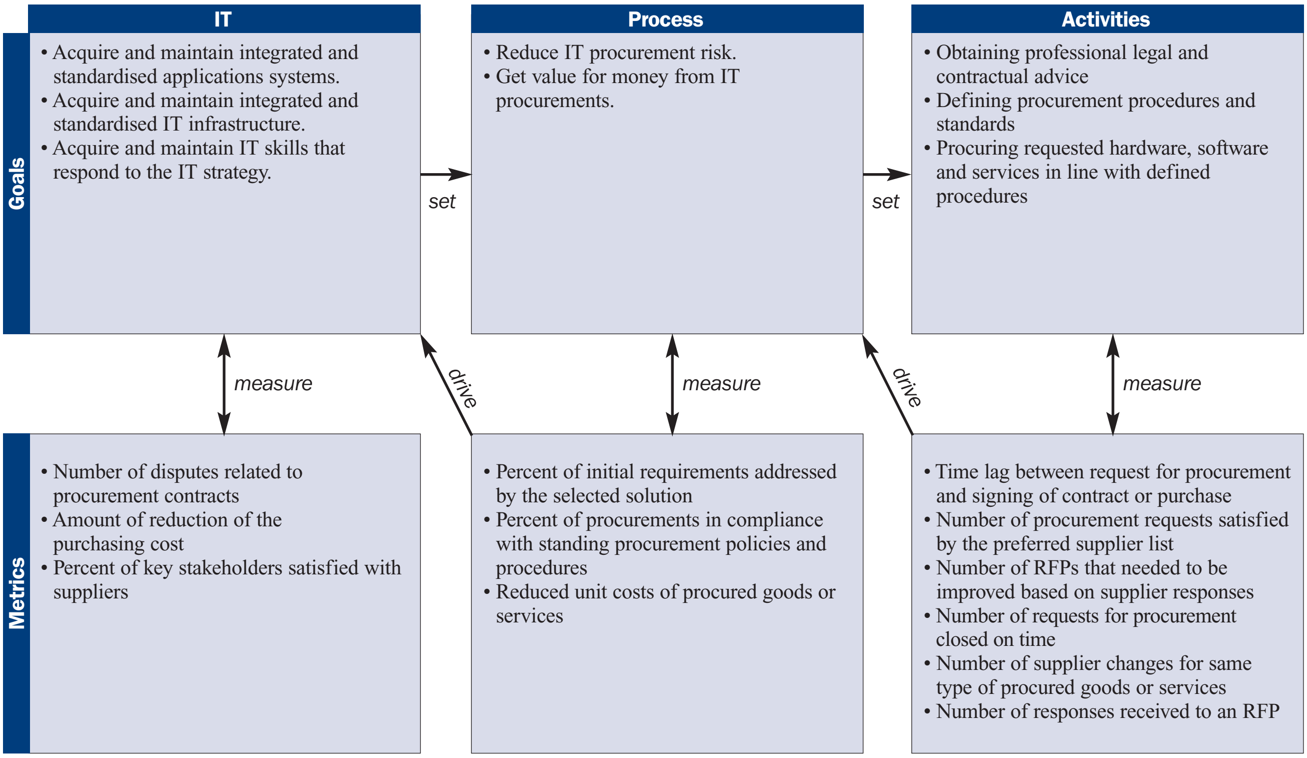
Outputs	To						
Third-party relationship management requirements	DS2						
Procured items	AI7						
Contractual arrangements	DS2						

RACI Chart

Activities	CEO	CFO	Business Executive	CIO	Business Process Owner	Head Operations	Chief Architect	Head Development	Head IT Administration	PMO	Compliance, Audit, Risk and Security
Develop IT procurement policies and procedures aligned with procurement policies at the corporate level.	I	C		A		I	I	I	R		C
Establish/maintain a list of accredited suppliers.									A/R		
Evaluate and select suppliers through a request for proposal (RFP) process.	C	C		A		R		R	R	R	C
Develop contracts that protect the organisation's interests.	R	C		A		R		R	R		C
Procure in compliance with established procedures.				A		R		R	R		C

A **RACI** chart identifies who is **R**esponsible, **A**ccountable, **C**onsulted and/or **I**nformed.

Goals and Metrics



IT

Goals:
- Acquire and maintain integrated and standardised applications systems.
- Acquire and maintain integrated and standardised IT infrastructure.
- Acquire and maintain IT skills that respond to the IT strategy.

Metrics:
- Number of disputes related to procurement contracts
- Amount of reduction of the purchasing cost
- Percent of key stakeholders satisfied with suppliers

Process

Goals:
- Reduce IT procurement risk.
- Get value for money from IT procurements.

Metrics:
- Percent of initial requirements addressed by the selected solution
- Percent of procurements in compliance with standing procurement policies and procedures
- Reduced unit costs of procured goods or services

Activities

Goals:
- Obtaining professional legal and contractual advice
- Defining procurement procedures and standards
- Procuring requested hardware, software and services in line with defined procedures

Metrics:
- Time lag between request for procurement and signing of contract or purchase
- Number of procurement requests satisfied by the preferred supplier list
- Number of RFPs that needed to be improved based on supplier responses
- Number of requests for procurement closed on time
- Number of supplier changes for same type of procured goods or services
- Number of responses received to an RFP

Maturity Model

AI5 Procure IT Resources

Management of the process of *Procure IT resources* that satisfies the business requirement for IT of *improving IT's cost-efficiency and its contribution to business profitability* is:

0 Non-existent when
There is no defined IT resource procurement process in place. The organisation does not recognise the need for clear procurement polices and procedures to ensure that all IT resources are available in a timely and cost-efficient manner.

1 Initial/*Ad Hoc* when
The organisation recognises the need to have documented policies and procedures that link IT acquisition to the business organisation's overall procurement process. Contracts for the acquisition of IT resources are developed and managed by project managers and other individuals exercising their professional judgement rather than as a result of formal procedures and policies. There is only an *ad hoc* relationship between corporate acquisition and contract management processes and IT. Contracts for acquisition are managed at the conclusion of projects rather than on a continuous basis.

2 Repeatable but Intuitive when
There is organisational awareness of the need to have basic policies and procedures for IT acquisition. Policies and procedures are partially integrated with the business organisation's overall procurement process. Procurement processes are mostly utilised for large and highly visible projects. Responsibilities and accountabilities for IT procurement and contract management are determined by the individual contract manager's experience. The importance of supplier management and relationship management is recognised; however, it is addressed based on individual initiative. Contract processes are mostly utilised by large or highly visible projects.

3 Defined when
Management institutes policies and procedures for IT acquisition. Policies and procedures are guided by the business organisation's overall procurement process. IT acquisition is largely integrated with overall business procurement systems. IT standards for the acquisition of IT resources exist. Suppliers of IT resources are integrated into the organisation's project management mechanisms from a contract management perspective. IT management communicates the need for appropriate acquisitions and contract management throughout the IT function.

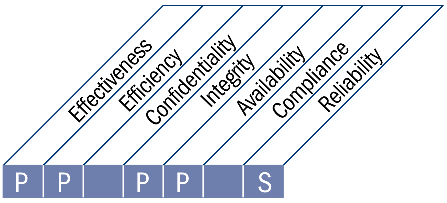
4 Managed and Measurable when
IT acquisition is fully integrated with overall business procurement systems. IT standards for the acquisition of IT resources are used for all procurements. Measurements on contract and procurement management are taken relevant to the business cases for IT acquisition. Reporting on IT acquisition activity that supports business objectives is available. Management is usually aware of exceptions to the policies and procedures for IT acquisition. Strategic management of relationships is developing. IT management enforces the use of the acquisition and contract management process for all acquisitions by reviewing performance measurement.

5 Optimised when
Management institutes resources' procurement thorough processes for IT acquisition. Management enforces compliance with policies and procedures for IT acquisition. Measurements on contract and procurement management are taken that are relevant to the business cases for IT acquisitions. Good relationships are established over time with most suppliers and partners, and the quality of relationships is measured and monitored. Relationships are managed strategically. IT standards, policies and procedures for the acquisition of IT resources are managed strategically and respond to measurement of the process. IT management communicates the strategic importance of appropriate acquisition and contract management throughout the IT function.

Process Description

AI6 Manage Changes

All changes, including emergency maintenance and patches, relating to infrastructure and applications within the production environment are formally managed in a controlled manner. Changes (including those to procedures, processes, system and service parameters) are logged, assessed and authorised prior to implementation and reviewed against planned outcomes following implementation. This assures mitigation of the risks of negatively impacting the stability or integrity of the production environment.



Plan and Organise
Acquire and Implement
Deliver and Support
Monitor and Evaluate

Control over the IT process of

Manage changes

that satisfies the business requirement for IT of

responding to business requirements in alignment with the business strategy, whilst reducing solution and service delivery defects and rework

by focusing on

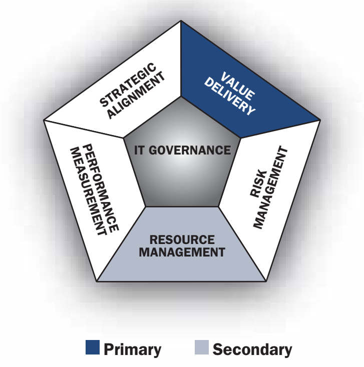
controlling impact assessment, authorisation and implementation of all changes to the IT infrastructure, applications and technical solutions; minimising errors due to incomplete request specifications; and halting implementation of unauthorised changes

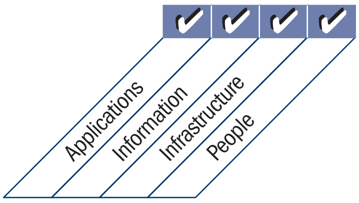
is achieved by

- Defining and communicating change procedures, including emergency changes
- Assessing, prioritising and authorising changes
- Tracking status and reporting on changes

and is measured by

- Number of disruptions or data errors caused by inaccurate specifications or incomplete impact assessment
- Amount of application or infrastructure rework caused by inadequate change specifications
- Percent of changes that follow formal change control processes





Control Objectives

AI6 Manage Changes

AI6.1 Change Standards and Procedures
Set up formal change management procedures to handle in a standardised manner all requests (including maintenance and patches) for changes to applications, procedures, processes, system and service parameters, and the underlying platforms.

AI6.2 Impact Assessment, Prioritisation and Authorisation
Assess all requests for change in a structured way to determine the impact on the operational system and its functionality. Ensure that changes are categorised, prioritised and authorised.

AI6.3 Emergency Changes
Establish a process for defining, raising, testing, documenting, assessing and authorising emergency changes that do not follow the established change process.

AI6.4 Change Status Tracking and Reporting
Establish a tracking and reporting system to document rejected changes, communicate the status of approved and in-process changes, and complete changes. Make certain that approved changes are implemented as planned.

AI6.5 Change Closure and Documentation
Whenever changes are implemented, update the associated system and user documentation and procedures accordingly.

Management Guidelines

AI6 Manage Changes

From	Inputs
PO1	IT project portfolio
PO8	Quality improvement actions
PO9	IT-related risk remedial action plans
PO10	Project management guidelines and detailed project plan
DS3	Required changes
DS5	Required security changes
DS8	Service requests/requests for change
DS9-10	Requests for change (where and how to apply the fix)
DS10	Problem records

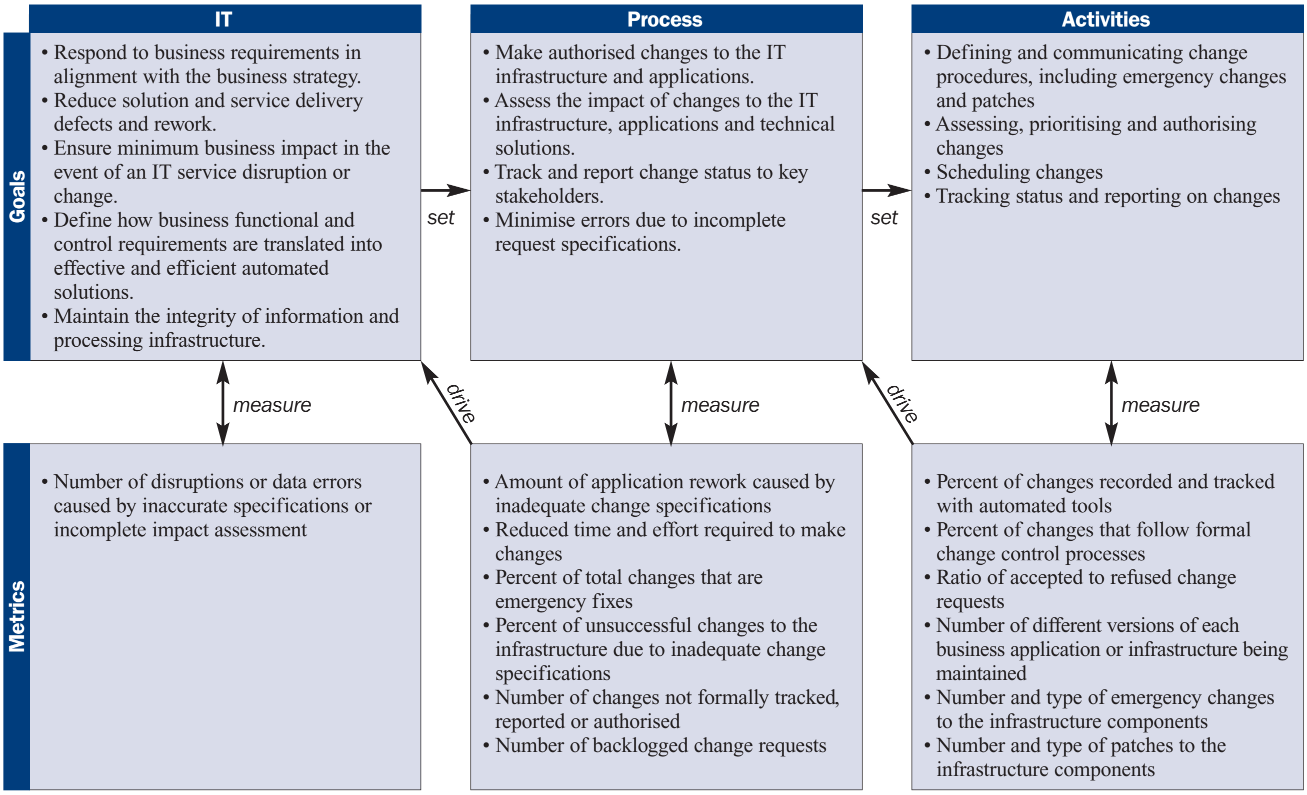
Outputs	To						
Change process description	AI1...AI3						
Change status reports	ME1						
Change authorisation	AI7	DS8	DS10				

RACI Chart

Activities \ Functions	CEO	CFO	Business Executive	CIO	Business Process Owner	Head Operations	Chief Architect	Head Development	Head IT Administration	PMO	Compliance, Audit, Risk and Security
Develop and implement a process to consistently record, assess and prioritise change requests.				A	I	R	C	R	C	C	C
Assess impact and prioritise changes based on business needs.				I	R	A/R	C	R	C	R	C
Assure that any emergency and critical change follows the approved process.				I	I	A/R	I	R			C
Authorise changes.				I	C	A/R		R			
Manage and disseminate relevant information regarding changes.				A	I	R	C	R	I	R	C

A **RACI** chart identifies who is **R**esponsible, **A**ccountable, **C**onsulted and/or **I**nformed.

Goals and Metrics



IT (Goals)

- Respond to business requirements in alignment with the business strategy.
- Reduce solution and service delivery defects and rework.
- Ensure minimum business impact in the event of an IT service disruption or change.
- Define how business functional and control requirements are translated into effective and efficient automated solutions.
- Maintain the integrity of information and processing infrastructure.

Process (Goals)

- Make authorised changes to the IT infrastructure and applications.
- Assess the impact of changes to the IT infrastructure, applications and technical solutions.
- Track and report change status to key stakeholders.
- Minimise errors due to incomplete request specifications.

Activities (Goals)

- Defining and communicating change procedures, including emergency changes and patches
- Assessing, prioritising and authorising changes
- Scheduling changes
- Tracking status and reporting on changes

IT (Metrics)

- Number of disruptions or data errors caused by inaccurate specifications or incomplete impact assessment

Process (Metrics)

- Amount of application rework caused by inadequate change specifications
- Reduced time and effort required to make changes
- Percent of total changes that are emergency fixes
- Percent of unsuccessful changes to the infrastructure due to inadequate change specifications
- Number of changes not formally tracked, reported or authorised
- Number of backlogged change requests

Activities (Metrics)

- Percent of changes recorded and tracked with automated tools
- Percent of changes that follow formal change control processes
- Ratio of accepted to refused change requests
- Number of different versions of each business application or infrastructure being maintained
- Number and type of emergency changes to the infrastructure components
- Number and type of patches to the infrastructure components

Maturity Model

AI6 Manage Changes

Management of the process of *Manage changes* that satisfies the business requirement for IT of *responding to business requirements in alignment with the business strategy, whilst reducing solution and service delivery defects and rework* is:

0 Non-existent when
There is no defined change management process, and changes can be made with virtually no control. There is no awareness that change can be disruptive for IT and business operations, and no awareness of the benefits of good change management.

1 Initial/*Ad Hoc* when
It is recognised that changes should be managed and controlled. Practices vary, and it is likely that unauthorised changes take place. There is poor or non-existent documentation of change, and configuration documentation is incomplete and unreliable. Errors are likely to occur together with interruptions to the production environment caused by poor change management.

2 Repeatable but Intuitive when
There is an informal change management process in place and most changes follow this approach; however, it is unstructured, rudimentary and prone to error. Configuration documentation accuracy is inconsistent, and only limited planning and impact assessment take place prior to a change.

3 Defined when
There is a defined formal change management process in place, including categorisation, prioritisation, emergency procedures, change authorisation and release management, and compliance is emerging. Workarounds take place, and processes are often bypassed. Errors may occur and unauthorised changes occasionally occur. The analysis of the impact of IT changes on business operations is becoming formalised, to support planned rollouts of new applications and technologies.

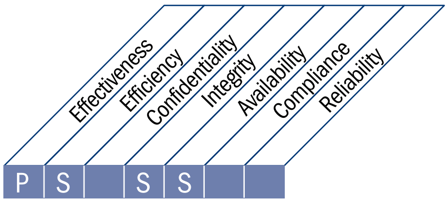
4 Managed and Measurable when
The change management process is well developed and consistently followed for all changes, and management is confident that there are minimal exceptions. The process is efficient and effective, but relies on considerable manual procedures and controls to ensure that quality is achieved. All changes are subject to thorough planning and impact assessment to minimise the likelihood of post-production problems. An approval process for changes is in place. Change management documentation is current and correct, with changes formally tracked. Configuration documentation is generally accurate. IT change management planning and implementation are becoming more integrated with changes in the business processes, to ensure that training, organisational changes and business continuity issues are addressed. There is increased co-ordination between IT change management and business process redesign. There is a consistent process for monitoring the quality and performance of the change management process.

5 Optimised when
The change management process is regularly reviewed and updated to stay in line with good practices. The review process reflects the outcome of monitoring. Configuration information is computer-based and provides version control. Tracking of changes is sophisticated and includes tools to detect unauthorised and unlicensed software. IT change management is integrated with business change management to ensure that IT is an enabler in increasing productivity and creating new business opportunities for the organisation.

Process Description

AI7 Install and Accredit Solutions and Changes

New systems need to be made operational once development is complete. This requires proper testing in a dedicated environment with relevant test data, definition of rollout and migration instructions, release planning and actual promotion to production, and a post-implementation review. This assures that operational systems are in line with the agreed-upon expectations and outcomes.



Plan and Organise
Acquire and Implement
Deliver and Support
Monitor and Evaluate

Control over the IT process of

Install and accredit solutions and changes

that satisfies the business requirement for IT of

implementing new or changed systems that work without major problems after installation

by focusing on

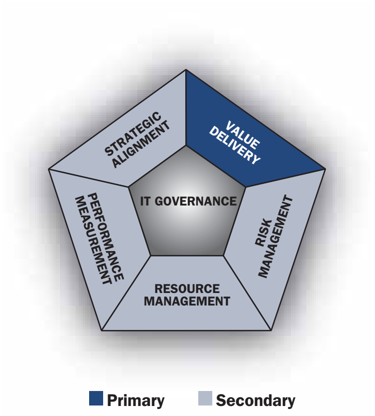
testing that applications and infrastructure solutions are fit for the intended purpose and free from errors, and planning releases to production

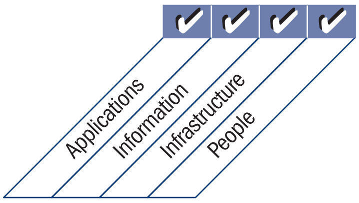
is achieved by

- Establishing test methodology
- Undertaking release planning
- Evaluating and approving test results by business management
- Performing post-implementation reviews

and is measured by

- Amount of application downtime or number of data fixes caused by inadequate testing
- Percent of systems that meet expected benefits as measured by the post-implementation process
- Percent of projects with a documented and approved testing plan





Control Objectives

AI7 Install and Accredit Solutions and Changes

AI7.1 Training
Train the staff members of the affected user departments and the operations group of the IT function in accordance with the defined training and implementation plan and associated materials, as part of every information systems development, implementation or modification project.

AI7.2 Test Plan
Establish a test plan based on organisationwide standards that defines roles, responsibilities, and entry and exit criteria. Ensure that the plan is approved by relevant parties.

AI7.3 Implementation Plan
Establish an implementation and fallback/backout plan. Obtain approval from relevant parties.

AI7.4 Test Environment
Define and establish a secure test environment representative of the planned operations environment relative to security, internal controls, operational practices, data quality and privacy requirements, and workloads.

AI7.5 System and Data Conversion
Plan data conversion and infrastructure migration as part of the organisation's development methods, including audit trails, rollbacks and fallbacks.

AI7.6 Testing of Changes
Test changes independently in accordance with the defined test plan prior to migration to the operational environment. Ensure that the plan considers security and performance.

AI7.7 Final Acceptance Test
Ensure that business process owners and IT stakeholders evaluate the outcome of the testing process as determined by the test plan. Remediate significant errors identified in the testing process, having completed the suite of tests identified in the test plan and any necessary regression tests. Following evaluation, approve promotion to production.

AI7.8 Promotion to Production
Following testing, control the handover of the changed system to operations, keeping it in line with the implementation plan. Obtain approval of the key stakeholders, such as users, system owner and operational management. Where appropriate, run the system in parallel with the old system for a while, and compare behaviour and results.

AI7.9 Post-implementation Review
Establish procedures in line with the organisational change management standards to require a post-implementation review as set out in the implementation plan.

Management Guidelines

AI7 Install and Accredit Solutions and Changes

From	Inputs
PO3	Technology standards
PO4	Documented system owners
PO8	Development standards
PO10	Project management guidelines and a detailed project plan
AI3	Configured system to be tested/installed
AI4	User, operational, support, technical and administration manuals
AI5	Procured items
AI6	Change authorisation

Outputs	To						
Released configuration items	DS8	DS9					
Known and accepted errors	AI4						
Promotion to production	DS13						
Software release and distribution plan	DS13						
Post-implementation review	PO2	PO5	PO10				
Internal control monitoring	ME2						

RACI Chart

Activities \ Functions	CEO	CFO	Business Executive	CIO	Business Process Owner	Head Operations	Chief Architect	Head Development	Head IT Administration	PMO	Compliance, Audit, Risk and Security
Build and review implementation plans.			C	A	I	C	C	R		C	C
Define and review a test strategy (entry and exit criteria) and an operational test plan methodology.			C	A	C	C	C	R		C	C
Build and maintain a business and technical requirements repository and test cases for accredited systems.				A				R			
Perform system conversion and integration tests on test environment.			I	I	R	C	C	A/R		I	C
Deploy a test environment and conduct final acceptance tests.			I	I	R	A	C	A/R		I	C
Recommend promotion to production based on agreed-upon accreditation criteria.			I	R	A	R	C	R		I	C

A **RACI** chart identifies who is **R**esponsible, **A**ccountable, **C**onsulted and/or **I**nformed.

Goals and Metrics

Goals

IT

- Ensure that automated business transactions and information exchanges can be trusted.
- Reduce solution and service delivery defects and rework.
- Respond to business requirements in alignment with the business strategy.
- Ensure seamless integration of applications into business processes.
- Ensure proper use and performance of the applications and technology solutions.
- Ensure that IT services and the IT infrastructure can properly resist and recover from failure due to error, delivered attack or disaster.

set

Process

- Verify and confirm that applications and technology solutions are fit for the intended purpose.
- Release and properly distribute approved applications and technology solutions.
- Prepare business users and operations for using applications and technology solutions.
- Ensure that new business applications and changes to existing applications are free from errors.

set

Activities

- Establishing a test methodology that ensures sufficient acceptance testing prior to go-live
- Tracking changes to all configuration items
- Undertaking release planning
- Performing post-implementation reviews
- Evaluating and approving test results by business management

measure | drive | measure | drive | measure

Metrics

IT

- Percent of stakeholders satisfied with the data integrity of new systems
- Percent of systems that met expected benefits as measured by the post-implementation process

Process

- Number of errors found during internal or external audits regarding the installation and accreditation process
- Rework after implementation due to inadequate acceptance testing
- Service desk calls from users due to inadequate training
- Application downtime or data fixes caused by inadequate testing

Activities

- Degree of stakeholder involvement in the installation and accreditation process
- Percent of projects with a documented and approved testing plan
- Number of lessons learnt from post-implementation review
- Percent of errors found during QA review of installation and accreditation functions
- Number of changes without required management sign-off before implementation

Maturity Model

AI7 Install and Accredit Solutions and Changes

Management of the process of *Install and accredit solutions and changes* that satisfies the business requirement for IT of *implementing new or changed systems that work without major problems after installation* is:

0 Non-existent when
There is a complete lack of formal installation or accreditation processes, and neither senior management nor IT staff members recognise the need to verify that solutions are fit for the intended purpose.

1 Initial/*Ad Hoc* when
There is an awareness of the need to verify and confirm that implemented solutions serve the intended purpose. Testing is performed for some projects, but the initiative for testing is left to the individual project teams, and the approaches taken vary. Formal accreditation and sign-off are rare or non-existent.

2 Repeatable but Intuitive when
There is some consistency amongst the testing and accreditation approaches, but typically they are not based on any methodology. The individual development teams normally decide the testing approach, and there is usually an absence of integration testing. There is an informal approval process.

3 Defined when
A formal methodology relating to installation, migration, conversion and acceptance is in place. IT installation and accreditation processes are integrated into the system life cycle and automated to some extent. Training, testing and transition to production status and accreditation are likely to vary from the defined process, based on individual decisions. The quality of systems entering production is inconsistent, with new systems often generating a significant level of post-implementation problems.

4 Managed and Measurable when
The procedures are formalised and developed to be well organised and practical with defined test environments and accreditation procedures. In practice, all major changes to systems follow this formalised approach. Evaluation of meeting user requirements is standardised and measurable, producing metrics that can be effectively reviewed and analysed by management. The quality of systems entering production is satisfactory to management even with reasonable levels of post-implementation problems. Automation of the process is *ad hoc* and project-dependent. Management may be satisfied with the current level of efficiency despite the lack of post-implementaiton evaluation. The test system adequately reflects the live environment. Stress testing for new systems and regression testing for existing systems are applied for major projects.

5 Optimised when
The installation and accreditation processes have been refined to a level of good practice, based on the results of continuous improvement and refinement. IT installation and accreditation processes are fully integrated into the system life cycle and automated when appropriate, facilitating the most efficient training, testing and transition to production status of new systems. Well-developed test environments, problem registers and fault resolution processes ensure efficient and effective transition to the production environment. Accreditation usually takes place with no rework, and post-implementation problems are normally limited to minor corrections. Post-implementation reviews are standardised, with lessons learned channelled back into the process to ensure continuous quality improvement. Stress testing for new systems and regression testing for modified systems are consistently applied.

Deliver and Support

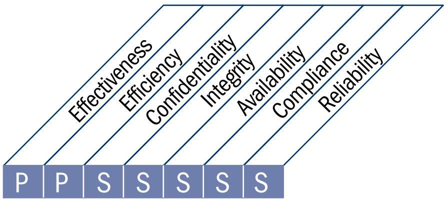
DS1	Define and Manage Service Levels
DS2	Manage Third-party Services
DS3	Manage Performance and Capacity
DS4	Ensure Continuous Service
DS5	Ensure Systems Security
DS6	Identify and Allocate Costs
DS7	Educate and Train Users
DS8	Manage Service Desk and Incidents
DS9	Manage the Configuration
DS10	Manage Problems
DS11	Manage Data
DS12	Manage the Physical Environment
DS13	Manage Operations

Deliver and Support

Process Description

DS1 Define and Manage Service Levels

Effective communication between IT management and business customers regarding services required is enabled by a documented definition of and agreement on IT services and service levels. This process also includes monitoring and timely reporting to stakeholders on the accomplishment of service levels. This process enables alignment between IT services and the related business requirements.



Plan and Organise
Acquire and Implement
Deliver and Support
Monitor and Evaluate

Control over the IT process of

Define and manage service levels

that satisfies the business requirement for IT of

ensuring the alignment of key IT services with the business strategy

by focusing on

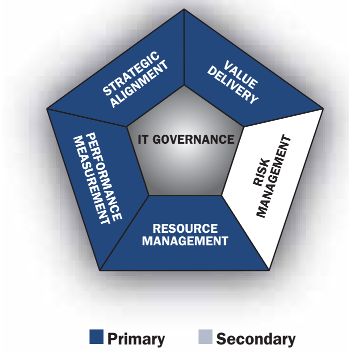
identifying service requirements, agreeing on service levels and monitoring the achievement of service levels

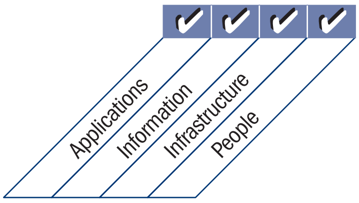
is achieved by

- Formalising internal and external agreements in line with requirements and delivery capabilities
- Reporting on service level achievements (reports and meetings)
- Identifying and communicating new and updated service requirements to strategic planning

and is measured by

- Percent of business stakeholders satisfied that service delivery meets agreed-upon levels
- Number of delivered services not in the catalogue
- Number of formal SLA review meetings with business customers per year





Control Objectives

DS1 Define and Manage Service Levels

DS1.1 Service Level Management Framework
Define a framework that provides a formalised service level management process between the customer and service provider. The framework should maintain continuous alignment with business requirements and priorities and facilitate common understanding between the customer and provider(s). The framework should include processes for creating service requirements, service definitions, SLAs, OLAs and funding sources. These attributes should be organised in a service catalogue. The framework should define the organisational structure for service level management, covering the roles, tasks and responsibilities of internal and external service providers and customers.

DS1.2 Definition of Services
Base definitions of IT services on service characteristics and business requirements. Ensure that they are organised and stored centrally via the implementation of a service catalogue portfolio approach.

DS1.3 Service Level Agreements
Define and agree to SLAs for all critical IT services based on customer requirements and IT capabilities. This should cover customer commitments; service support requirements; quantitative and qualitative metrics for measuring the service signed off on by the stakeholders; funding and commercial arrangements, if applicable; and roles and responsibilities, including oversight of the SLA. Consider items such as availability, reliability, performance, capacity for growth, levels of support, continuity planning, security and demand constraints.

DS1.4 Operating Level Agreements
Define OLAs that explain how the services will be technically delivered to support the SLA(s) in an optimal manner. The OLAs should specify the technical processes in terms meaningful to the provider and may support several SLAs.

DS1.5 Monitoring and Reporting of Service Level Achievements
Continuously monitor specified service level performance criteria. Reports on achievement of service levels should be provided in a format that is meaningful to the stakeholders. The monitoring statistics should be analysed and acted upon to identify negative and positive trends for individual services as well as for services overall.

DS1.6 Review of Service Level Agreements and Contracts
Regularly review SLAs and underpinning contracts (UCs) with internal and external service providers to ensure that they are effective and up to date and that changes in requirements have been taken into account.

Management Guidelines

DS1 Define and Manage Service Levels

From	Inputs
PO1	Strategic and tactical IT plans, IT service portfolio
PO2	Assigned data classifications
PO5	Updated IT service portfolio
AI2	Initial planned SLAs
AI3	Initial planned OLAs
DS4	Disaster service requirements, including roles and responsibilities
ME1	Performance input to IT planning

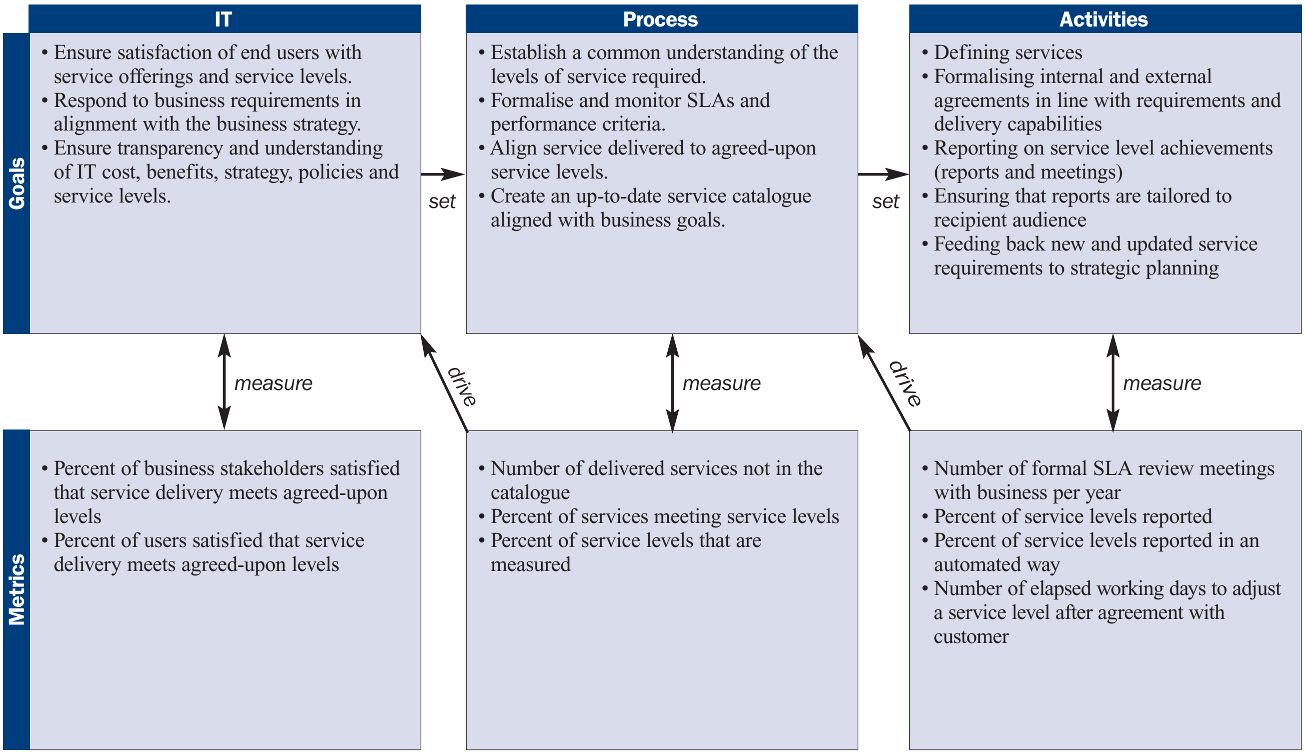
Outputs	To						
Contract review report	DS2						
Process performance reports	ME1						
New/updated service requirements	PO1						
SLAs	AI1	DS2	DS3	DS4	DS6	DS8	DS13
OLAs	DS4	DS5	DS6	DS7	DS8	DS11	DS13
Updated IT service portfolio	PO1						

RACI Chart

Activities / Functions	CEO	CFO	Business Executive	CIO	Business Process Owner	Head Operations	Chief Architect	Head Development	Head IT Administration	PMO	Compliance, Audit, Risk and Security	Service Manager
Create a framework for defining IT services.			C	A	C	C	I	C	C	I	C	R
Build an IT service catalogue.			I	A	C	C	I	C	C	I	I	R
Define SLAs for critical IT services.		I	I	C	C	R	I	R	R	C	C	A/R
Define OLAs for meeting SLAs.				I	C	R	I	R	R	C	C	A/R
Monitor and report end-to-end service level performance.				I	I	R		I	I		I	A/R
Review SLAs and UCs.		I		I	C	R		R	R		C	A/R
Review and update IT service catalogue.			I	A	C	C	I	C	C	I	I	R
Create service improvement plan.			I	A	I	R	I	R	C	C	I	R

A **RACI** chart identifies who is **R**esponsible, **A**ccountable, **C**onsulted and/or **I**nformed.

Goals and Metrics



IT

Goals:
- Ensure satisfaction of end users with service offerings and service levels.
- Respond to business requirements in alignment with the business strategy.
- Ensure transparency and understanding of IT cost, benefits, strategy, policies and service levels.

Metrics:
- Percent of business stakeholders satisfied that service delivery meets agreed-upon levels
- Percent of users satisfied that service delivery meets agreed-upon levels

Process

Goals:
- Establish a common understanding of the levels of service required.
- Formalise and monitor SLAs and performance criteria.
- Align service delivered to agreed-upon service levels.
- Create an up-to-date service catalogue aligned with business goals.

Metrics:
- Number of delivered services not in the catalogue
- Percent of services meeting service levels
- Percent of service levels that are measured

Activities

Goals:
- Defining services
- Formalising internal and external agreements in line with requirements and delivery capabilities
- Reporting on service level achievements (reports and meetings)
- Ensuring that reports are tailored to recipient audience
- Feeding back new and updated service requirements to strategic planning

Metrics:
- Number of formal SLA review meetings with business per year
- Percent of service levels reported
- Percent of service levels reported in an automated way
- Number of elapsed working days to adjust a service level after agreement with customer

Maturity Model

DS1 Define and Manage Service Levels

Management of the process of *Define and manage service levels* that satisfies the business requirement for IT of *ensuring the alignment of key IT services with the business strategy* is:

0 Non-existent when
Management has not recognised the need for a process for defining service levels. Accountabilities and responsibilities for monitoring them are not assigned.

1 Initial/*Ad Hoc* when
There is awareness of the need to manage service levels, but the process is informal and reactive. The responsibility and accountability for defining and managing services are not defined. If performance measurements exist, they are qualitative only with imprecisely defined goals. Reporting is informal, infrequent and inconsistent.

2 Repeatable but Intuitive when
There are agreed-upon service levels, but they are informal and not reviewed. Service level reporting is incomplete and may be irrelevant or misleading for customers. Service level reporting is dependent on the skills and initiative of individual managers. A service level co-ordinator is appointed with defined responsibilities, but limited authority. If a process for compliance to SLAs exists, it is voluntary and not enforced.

3 Defined when
Responsibilities are well defined, but with discretionary authority. The SLA development process is in place with checkpoints for reassessing service levels and customer satisfaction. Services and service levels are defined, documented and agreed-upon using a standard process. Service level shortfalls are identified, but procedures on how to resolve shortfalls are informal. There is a clear linkage between expected service level achievement and the funding provided. Service levels are agreed to, but they may not address business needs.

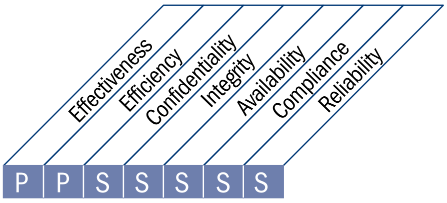
4 Managed and Measurable when
Service levels are increasingly defined in the system requirements definition phase and incorporated into the design of the application and operational environments. Customer satisfaction is routinely measured and assessed. Performance measures reflect customer needs, rather than IT goals. The measures for assessing service levels are becoming standardised and reflect industry norms. The criteria for defining service levels are based on business criticality and include availability, reliability, performance, growth capacity, user support, continuity planning and security considerations. Root cause analysis is routinely performed when service levels are not met. The reporting process for monitoring service levels is becoming increasingly automated. Operational and financial risks associated with not meeting agreed-upon service levels are defined and clearly understood. A formal system of measurement is instituted and maintained.

5 Optimised when
Service levels are continuously re-evaluated to ensure alignment of IT and business objectives, whilst taking advantage of technology, including the cost-benefit ratio. All service level management processes are subject to continuous improvement. Customer satisfaction levels are continuously monitored and managed. Expected service levels reflect strategic goals of business units and are evaluated against industry norms. IT management has the resources and accountability needed to meet service level targets, and compensation is structured to provide incentives for meeting these targets. Senior management monitors performance metrics as part of a continuous improvement process.

Process Description

DS2 Manage Third-party Services

The need to assure that services provided by third parties (suppliers, vendors and partners) meet business requirements requires an effective third-party management process. This process is accomplished by clearly defining the roles, responsibilities and expectations in third-party agreements as well as reviewing and monitoring such agreements for effectiveness and compliance. Effective management of third-party services minimises the business risk associated with non-performing suppliers.



Control over the IT process of

Manage third-party services

that satisfies the business requirement for IT of

providing satisfactory third-party services whilst being transparent about benefits, costs and risks

by focusing on

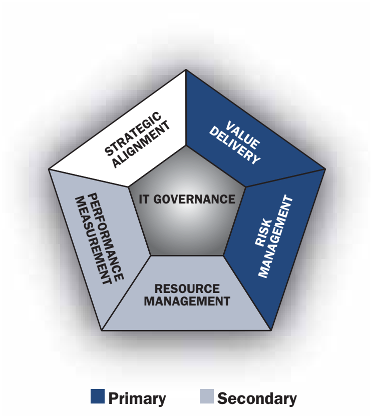
establishing relationships and bilateral responsibilities with qualified third-party service providers and monitoring the service delivery to verify and ensure adherence to agreements

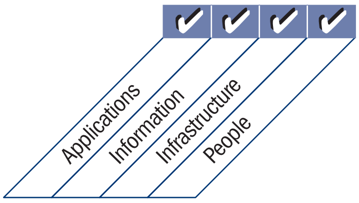
is achieved by

- Identifying and categorising supplier services
- Identifying and mitigating supplier risk
- Monitoring and measuring supplier performance

and is measured by

- Number of user complaints due to contracted services
- Percent of major suppliers meeting clearly defined requirements and service levels
- Percent of major suppliers subject to monitoring





Control Objectives

DS2 Manage Third-party Services

DS2.1 Identification of All Supplier Relationships

Identify all supplier services, and categorise them according to supplier type, significance and criticality. Maintain formal documentation of technical and organisational relationships covering the roles and responsibilities, goals, expected deliverables, and credentials of representatives of these suppliers.

DS2.2 Supplier Relationship Management

Formalise the supplier relationship management process for each supplier. The relationship owners should liaise on customer and supplier issues and ensure the quality of the relationship based on trust and transparency (e.g., through SLAs).

DS2.3 Supplier Risk Management

Identify and mitigate risks relating to suppliers' ability to continue effective service delivery in a secure and efficient manner on a continual basis. Ensure that contracts conform to universal business standards in accordance with legal and regulatory requirements. Risk management should further consider non-disclosure agreements (NDAs), escrow contracts, continued supplier viability, conformance with security requirements, alternative suppliers, penalties and rewards, etc.

DS2.4 Supplier Performance Monitoring

Establish a process to monitor service delivery to ensure that the supplier is meeting current business requirements and continuing to adhere to the contract agreements and SLAs, and that performance is competitive with alternative suppliers and market conditions.

Management Guidelines

DS2 Manage Third-party Services

From	Inputs
PO1	IT sourcing strategy
PO8	Acquisition standards
AI5	Contractual arrangements, third-party relationship management requirements
DS1	SLAs, contract review report
DS4	Disaster service requirements, including roles and responsibilities

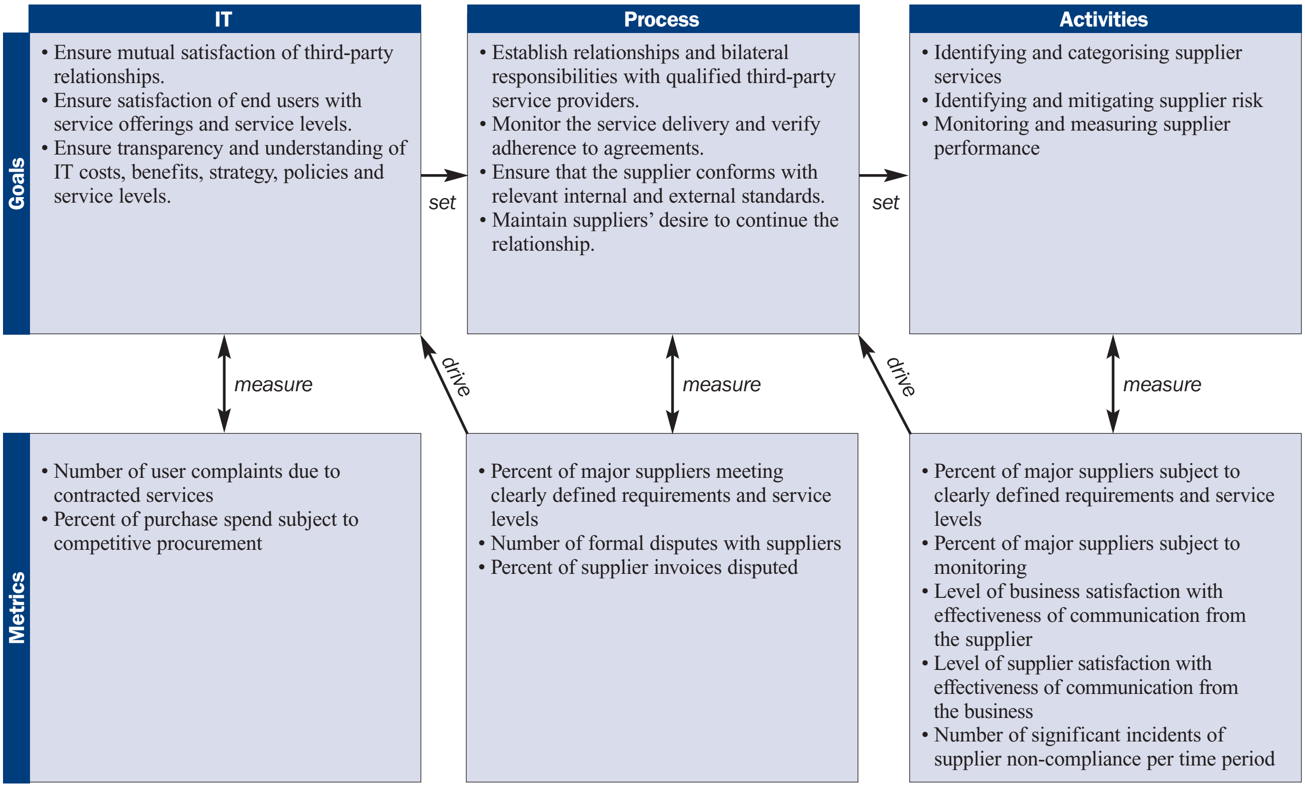
Outputs	To						
Process performance reports	ME1						
Supplier catalogue	AI5						
Supplier risks	PO9						

RACI Chart

Activities \ Functions	CEO	CFO	Business Executive	CIO	Business Process Owner	Head Operations	Chief Architect	Head Development	Head IT Administration	PMO	Compliance, Audit, Risk and Security
Identify and categorise third-party service relationships.				I	C	R	C	R	A/R	C	C
Define and document supplier management processes.		C		A	I	R	I	R	R	C	C
Establish supplier evaluation and selection policies and procedures.		C		A	C	C		C	R	C	C
Identify, assess and mitigate supplier risks.		I		A		R		R	R	C	C
Monitor supplier service delivery.				R	A	R		R	R	C	C
Evaluate long-term goals of the service relationship for all stakeholders.	C	C	C	A/R	C	C	C	C	R	C	C

A **RACI** chart identifies who is **R**esponsible, **A**ccountable, **C**onsulted and/or **I**nformed.

Goals and Metrics



IT – Goals
- Ensure mutual satisfaction of third-party relationships.
- Ensure satisfaction of end users with service offerings and service levels.
- Ensure transparency and understanding of IT costs, benefits, strategy, policies and service levels.

Process – Goals
- Establish relationships and bilateral responsibilities with qualified third-party service providers.
- Monitor the service delivery and verify adherence to agreements.
- Ensure that the supplier conforms with relevant internal and external standards.
- Maintain suppliers' desire to continue the relationship.

Activities – Goals
- Identifying and categorising supplier services
- Identifying and mitigating supplier risk
- Monitoring and measuring supplier performance

IT – Metrics
- Number of user complaints due to contracted services
- Percent of purchase spend subject to competitive procurement

Process – Metrics
- Percent of major suppliers meeting clearly defined requirements and service levels
- Number of formal disputes with suppliers
- Percent of supplier invoices disputed

Activities – Metrics
- Percent of major suppliers subject to clearly defined requirements and service levels
- Percent of major suppliers subject to monitoring
- Level of business satisfaction with effectiveness of communication from the supplier
- Level of supplier satisfaction with effectiveness of communication from the business
- Number of significant incidents of supplier non-compliance per time period

Maturity Model

DS2 Manage Third-party Services

Management of the process of *Manage third-party services* that satisfies the business requirement for IT of *providing satisfactory third-party services whilst being transparent about benefits, costs and risks* is:

0 Non-existent when
Responsibilities and accountabilities are not defined. There are no formal policies and procedures regarding contracting with third parties. Third-party services are neither approved nor reviewed by management. There are no measurement activities and no reporting by third parties. In the absence of a contractual obligation for reporting, senior management is not aware of the quality of the service delivered.

1 Initial/*Ad Hoc* when
Management is aware of the need to have documented policies and procedures for third-party management, including signed contracts. There are no standard terms of agreement with service providers. Measurement of the services provided is informal and reactive. Practices are dependent on the experience (e.g., on demand) of the individual and the supplier.

2 Repeatable but Intuitive when
The process for overseeing third-party service providers, associated risks and the delivery of services is informal. A signed, *pro forma* contract is used with standard vendor terms and conditions (e.g., the description of services to be provided). Reports on the services provided are available, but do not support business objectives.

3 Defined when
Well-documented procedures are in place to govern third-party services, with clear processes for vetting and negotiating with vendors. When an agreement for the provision of services is made, the relationship with the third party is purely a contractual one. The nature of the services to be provided is detailed in the contract and includes legal, operational and control requirements. The responsibility for oversight of third-party services is assigned. Contractual terms are based on standardised templates. The business risk associated with the third-party services is assessed and reported.

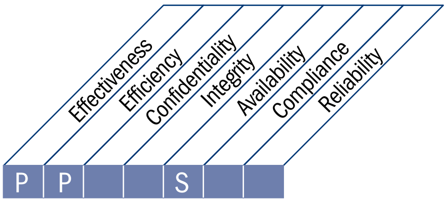
4 Managed and Measurable when
Formal and standardised criteria are established for defining the terms of engagement, including scope of work, services/deliverables to be provided, assumptions, schedule, costs, billing arrangements and responsibilities. Responsibilities for contract and vendor management are assigned. Vendor qualifications, risks and capabilities are verified on a continual basis. Service requirements are defined and linked to business objectives. A process exists to review service performance against contractual terms, providing input to assess current and future third-party services. Transfer pricing models are used in the procurement process. All parties involved are aware of service, cost and milestone expectations. Agreed-upon goals and metrics for the oversight of service providers exist.

5 Optimised when
Contracts signed with third parties are reviewed periodically at predefined intervals. The responsibility for managing suppliers and the quality of the services provided is assigned. Evidence of contract compliance to operational, legal and control provisions is monitored, and corrective action is enforced. The third party is subject to independent periodic review, and feedback on performance is provided and used to improve service delivery. Measurements vary in response to changing business conditions. Measures support early detection of potential problems with third-party services. Comprehensive, defined reporting of service level achievement is linked to the third-party compensation. Management adjusts the process of third-party service acquisition and monitoring based on the measurers.

Process Description

DS3 Manage Performance and Capacity

The need to manage performance and capacity of IT resources requires a process to periodically review current performance and capacity of IT resources. This process includes forecasting future needs based on workload, storage and contingency requirements. This process provides assurance that information resources supporting business requirements are continually available.



Control over the IT process of

Manage performance and capacity

that satisfies the business requirement for IT of

optimising the performance of IT infrastructure, resources and capabilities in response to business needs

by focusing on

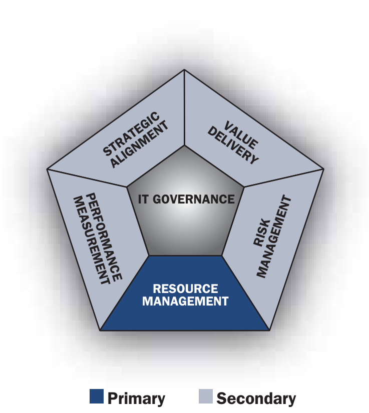
meeting response time requirements of SLAs, minimising downtime, and making continuous IT performance and capacity improvements through monitoring and measurement

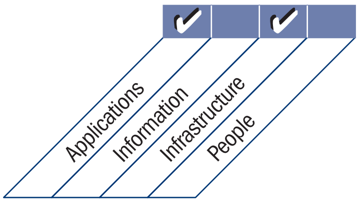
is achieved by

- Planning and providing system capacity and availability
- Monitoring and reporting system performance
- Modelling and forecasting system performance

and is measured by

- Number of hours lost per user per month due to insufficient capacity planning
- Percent of peaks where target utilisation is exceeded
- Percent of response-time SLAs not met





Control Objectives

DS3 Manage Performance and Capacity

DS3.1 Performance and Capacity Planning
Establish a planning process for the review of performance and capacity of IT resources to ensure that cost-justifiable capacity and performance are available to process the agreed-upon workloads as determined by the SLAs. Capacity and performance plans should leverage appropriate modelling techniques to produce a model of the current and forecasted performance, capacity and throughput of the IT resources.

DS3.2 Current Performance and Capacity
Assess current performance and capacity of IT resources to determine if sufficient capacity and performance exist to deliver against agreed-upon service levels.

DS3.3 Future Performance and Capacity
Conduct performance and capacity forecasting of IT resources at regular intervals to minimise the risk of service disruptions due to insufficient capacity or performance degradation, and identify excess capacity for possible redeployment. Identify workload trends and determine forecasts to be input to performance and capacity plans.

DS3.4 IT Resources Availability
Provide the required capacity and performance, taking into account aspects such as normal workloads, contingencies, storage requirements and IT resource life cycles. Provisions such as prioritising tasks, fault-tolerance mechanisms and resource allocation practices should be made. Management should ensure that contingency plans properly address availability, capacity and performance of individual IT resources.

DS3.5 Monitoring and Reporting
Continuously monitor the performance and capacity of IT resources. Data gathered should serve two purposes:

- To maintain and tune current performance within IT and address such issues as resilience, contingency, current and projected workloads, storage plans, and resource acquisition
- To report delivered service availability to the business, as required by the SLAs

Accompany all exception reports with recommendations for corrective action.

Management Guidelines

DS3 Manage Performance and Capacity

From	Inputs
AI2	Availability, continuity and recovery specification
AI3	System monitoring requirements
DS1	SLAs

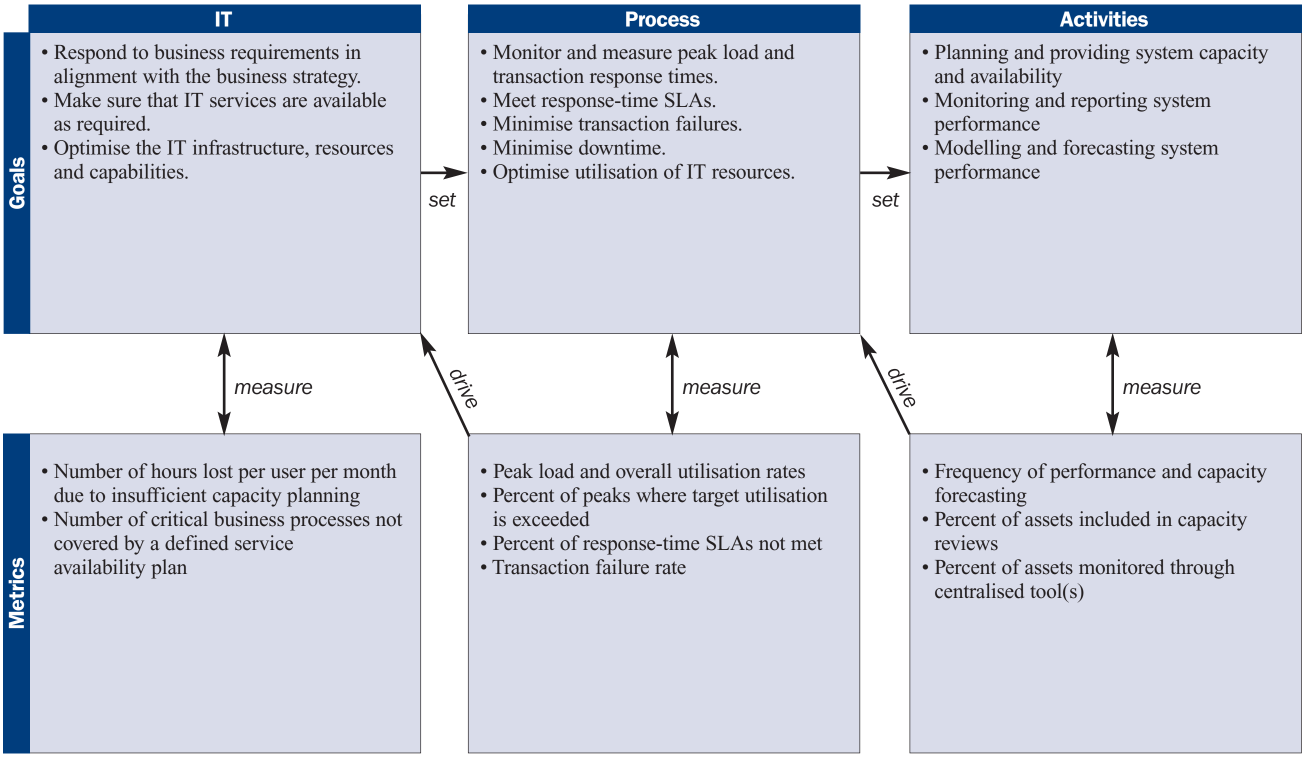
Outputs	To						
Performance and capacity information	PO2	PO3					
Performance and capacity plan (requirements)	PO5	AI1	AI3	ME1			
Required changes	AI6						
Process performance reports	ME1						

RACI Chart

Activities	CEO	CFO	Business Executive	CIO	Business Process Owner	Head Operations	Chief Architect	Head Development	Head IT Administration	PMO	Compliance, Audit, Risk and Security
Establish a planning process for the review of performance and capacity of IT resources.				A		R	C	C	C	C	
Review current IT resources' performance and capacity.				C	I	A/R		C	C	C	
Conduct IT resources' performance and capacity forecasting.				C	C	A/R	C	C	C	C	
Conduct gap analysis to identify IT resources mismatches.				C	I	A/R		R	C	C	I
Conduct contingency planning for potential IT resources unavailability.				C	I	A/R		C	C	I	C
Continuously monitor and report the availability, performance and capacity of IT resources.				I	I	A/R		I	I	I	I

A **RACI** chart identifies who is **R**esponsible, **A**ccountable, **C**onsulted and/or **I**nformed.

Goals and Metrics



Goals – IT
- Respond to business requirements in alignment with the business strategy.
- Make sure that IT services are available as required.
- Optimise the IT infrastructure, resources and capabilities.

Goals – Process
- Monitor and measure peak load and transaction response times.
- Meet response-time SLAs.
- Minimise transaction failures.
- Minimise downtime.
- Optimise utilisation of IT resources.

Goals – Activities
- Planning and providing system capacity and availability
- Monitoring and reporting system performance
- Modelling and forecasting system performance

Metrics – IT
- Number of hours lost per user per month due to insufficient capacity planning
- Number of critical business processes not covered by a defined service availability plan

Metrics – Process
- Peak load and overall utilisation rates
- Percent of peaks where target utilisation is exceeded
- Percent of response-time SLAs not met
- Transaction failure rate

Metrics – Activities
- Frequency of performance and capacity forecasting
- Percent of assets included in capacity reviews
- Percent of assets monitored through centralised tool(s)

Maturity Model

DS3 Manage Performance and Capacity

Management of the process of *Manage performance and capacity* that satisfies the business requirement for IT of *optimising the performance of IT infrastructure, resources and capabilities in response to business needs* is:

0 Non-existent when
Management does not recognise that key business processes may require high levels of performance from IT or that the overall business need for IT services may exceed capacity. There is no capacity planning process in place.

1 Initial/*Ad Hoc* when
Users devise workarounds for performance and capacity constraints. There is very little appreciation of the need for capacity and performance planning by the owners of the business processes. Action taken toward managing performance and capacity is typically reactive. The process for planning capacity and performance is informal. The understanding of current and future capacity and performance of IT resources is limited.

2 Repeatable but Intuitive when
Business and IT management are aware of the impact of not managing performance and capacity. Performance needs are generally met based on assessments of individual systems and the knowledge of support and project teams. Some individual tools may be used to diagnose performance and capacity problems, but the consistency of results is dependent on the expertise of key individuals. There is no overall assessment of the IT performance capability or consideration of peak and worst-case loading situations. Availability problems are likely to occur in an unexpected and random fashion and take considerable time to diagnose and correct. Any performance measurement is based primarily on IT needs and not on customer needs.

3 Defined when
Performance and capacity requirements are defined throughout the system life cycle. There are defined service level requirements and metrics that can be used to measure operational performance. Future performance and capacity requirements are modelled following a defined process. Reports are produced giving performance statistics. Performance- and capacity-related problems are still likely to occur and be time-consuming to correct. Despite published service levels, users and customers may feel sceptical about the service capability.

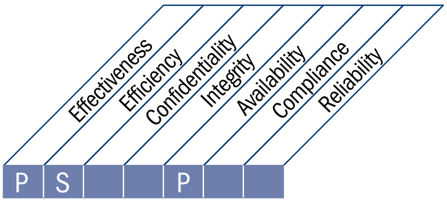
4 Managed and Measurable when
Processes and tools are available to measure system usage, performance and capacity, and results are compared to defined goals. Up-to-date information is available, giving standardised performance statistics and alerting incidents caused by insufficient performance and capacity. Insufficient performance and capacity issues are dealt with according to defined and standardised procedures. Automated tools are used to monitor specific resources, such as disk space, networks, servers and network gateways. Performance and capacity statistics are reported in business process terms, so users and customers understand IT service levels. Users feel generally satisfied with the current service capability and may demand new and improved availability levels. Metrics for measuring IT performance and capacity are agreed upon but may be only sporadically and inconsistently applied.

5 Optimised when
The performance and capacity plans are fully synchronised with the business demand forecasts. The IT infrastructure and business demand are subject to regular reviews to ensure that optimum capacity is achieved at the lowest possible cost. Tools for monitoring critical IT resources are standardised and used across platforms and linked to an organisationwide incident management system. Monitoring tools detect and can automatically correct performance- and capacity-related issues. Trend analysis is performed and shows imminent performance problems caused by increased business volumes, enabling planning and avoidance of unexpected issues. Metrics for measuring IT performance and capacity have been fine-tuned into outcome measures and performance indicators for all critical business processes and are consistently measured. Management adjusts the planning for performance and capacity following analysis of these measures.

Process Description

DS4 Ensure Continuous Service

The need for providing continuous IT services requires developing, maintaining and testing IT continuity plans, utilising offsite backup storage and providing periodic continuity plan training. An effective continuous service process minimises the probability and impact of a major IT service interruption on key business functions and processes.



Control over the IT process of

Ensure continuous service

that satisfies the business requirement for IT of

ensuring minimal business impact in the event of an IT service interruption

by focusing on

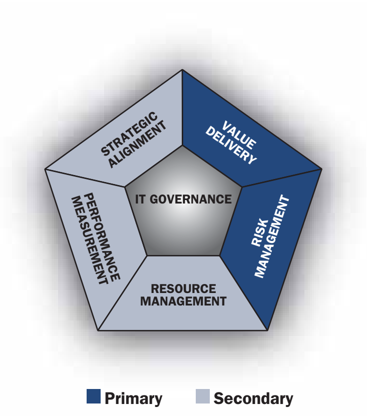
building resilience into automated solutions and developing, maintaining and testing IT continuity plans

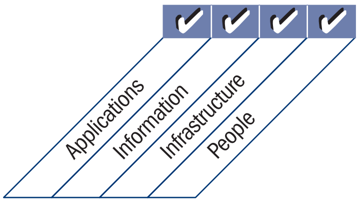
is achieved by

- Developing and maintaining (improving) IT contingency
- Training on and testing IT contingency plans
- Storing copies of contingency plans and data at offsite locations

and is measured by

- Number of hours lost per user per month due to unplanned outages
- Number of business-critical processes relying on IT not covered by the IT continuity plan





Control Objectives

DS4 Ensure Continuous Service

DS4.1 IT Continuity Framework

Develop a framework for IT continuity to support enterprisewide business continuity management using a consistent process. The objective of the framework should be to assist in determining the required resilience of the infrastructure and to drive the development of disaster recovery and IT contingency plans. The framework should address the organisational structure for continuity management, covering the roles, tasks and responsibilities of internal and external service providers, their management and their customers, and the planning processes that create the rules and structures to document, test and execute the disaster recovery and IT contingency plans. The plan should also address items such as the identification of critical resources, noting key dependencies, the monitoring and reporting of the availability of critical resources, alternative processing, and the principles of backup and recovery.

DS4.2 IT Continuity Plans

Develop IT continuity plans based on the framework and designed to reduce the impact of a major disruption on key business functions and processes. The plans should be based on risk understanding of potential business impacts and address requirements for resilience, alternative processing and recovery capability of all critical IT services. They should also cover usage guidelines, roles and responsibilities, procedures, communication processes, and the testing approach.

DS4.3 Critical IT Resources

Focus attention on items specified as most critical in the IT continuity plan to build in resilience and establish priorities in recovery situations. Avoid the distraction of recovering less-critical items and ensure response and recovery in line with prioritised business needs, while ensuring that costs are kept at an acceptable level and complying with regulatory and contractual requirements. Consider resilience, response and recovery requirements for different tiers, e.g., one to four hours, four to 24 hours, more than 24 hours and critical business operational periods.

DS4.4 Maintenance of the IT Continuity Plan

Encourage IT management to define and execute change control procedures to ensure that the IT continuity plan is kept up to date and continually reflects actual business requirements. Communicate changes in procedures and responsibilities clearly and in a timely manner.

DS4.5 Testing of the IT Continuity Plan

Test the IT continuity plan on a regular basis to ensure that IT systems can be effectively recovered, shortcomings are addressed and the plan remains relevant. This requires careful preparation, documentation, reporting of test results and, according to the results, implementation of an action plan. Consider the extent of testing recovery of single applications to integrated testing scenarios to end-to-end testing and integrated vendor testing.

DS4.6 IT Continuity Plan Training

Provide all concerned parties with regular training sessions regarding the procedures and their roles and responsibilities in case of an incident or disaster. Verify and enhance training according to the results of the contingency tests.

DS4.7 Distribution of the IT Continuity Plan

Determine that a defined and managed distribution strategy exists to ensure that plans are properly and securely distributed and available to appropriately authorised interested parties when and where needed. Attention should be paid to making the plans accessible under all disaster scenarios.

DS4.8 IT Services Recovery and Resumption

Plan the actions to be taken for the period when IT is recovering and resuming services. This may include activation of backup sites, initiation of alternative processing, customer and stakeholder communication, and resumption procedures. Ensure that the business understands IT recovery times and the necessary technology investments to support business recovery and resumption needs.

DS4.9 Offsite Backup Storage

Store offsite all critical backup media, documentation and other IT resources necessary for IT recovery and business continuity plans. Determine the content of backup storage in collaboration between business process owners and IT personnel. Management of the offsite storage facility should respond to the data classification policy and the enterprise's media storage practices. IT management should ensure that offsite arrangements are periodically assessed, at least annually, for content, environmental protection and security. Ensure compatibility of hardware and software to restore archived data, and periodically test and refresh archived data.

DS4.10 Post-resumption Review

Determine whether IT management has established procedures for assessing the adequacy of the plan in regard to the successful resumption of the IT function after a disaster, and update the plan accordingly.

Management Guidelines

DS4 Ensure Continuous Service

From	Inputs
PO2	Assigned data classifications
PO9	Risk assessment
AI2	Availability, continuity and recovery specification
AI4	User, operational, support, technical and administration manuals
DS1	SLAs and OLAs

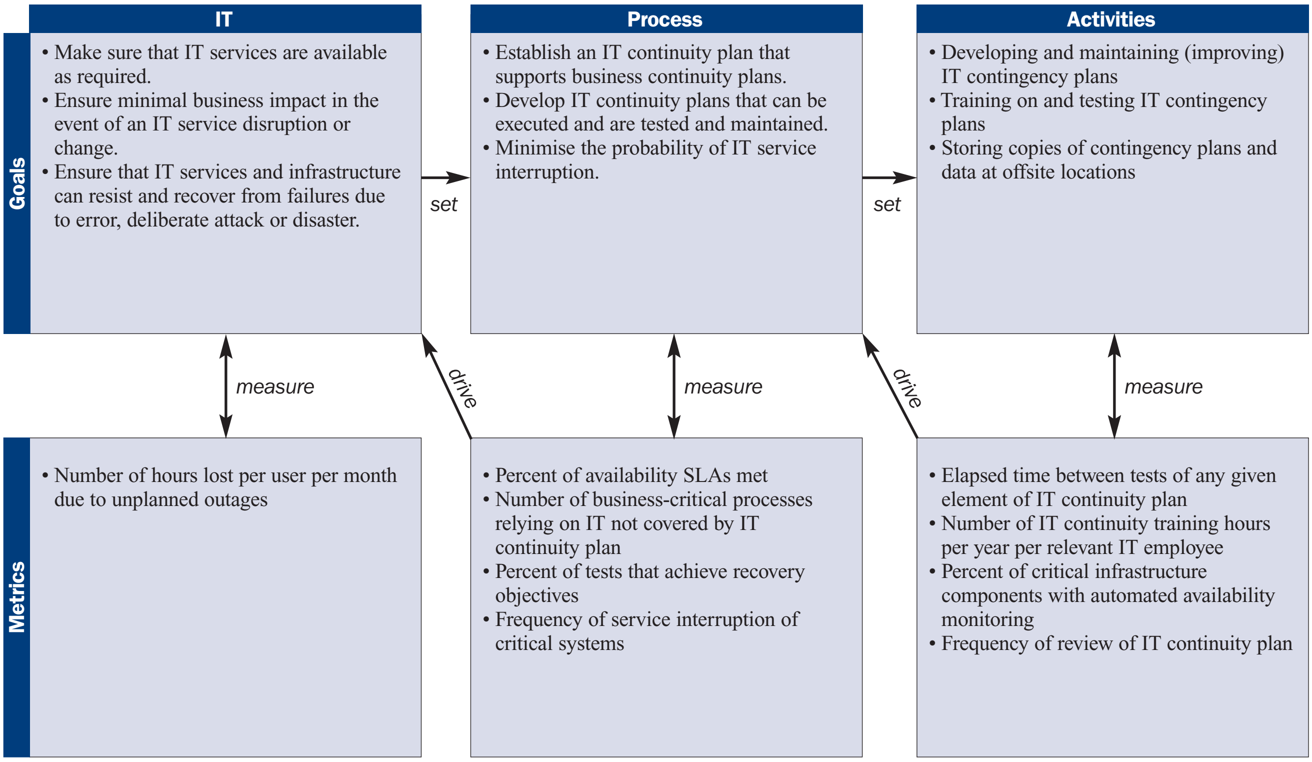
Outputs	To						
Contingency test results	PO9						
Criticality of IT configuration items	DS9						
Backup storage and protection plan	DS11	DS13					
Incident/disaster thresholds	DS8						
Disaster service requirements, including roles and responsibilities	DS1	DS2					
Process performance reports	ME1						

RACI Chart

Activities	CEO	CFO	Business Executive	CIO	Business Process Owner	Head Operations	Chief Architect	Head Development	Head IT Administration	PMO	Compliance, Audit, Risk and Security
Develop an IT continuity framework.		C	C	A	C	R	R	R	C	C	R
Conduct a business impact analysis and risk assessment.		C	C	C	C	A/R	C	C	C	C	C
Develop and maintain IT continuity plans.	I	C	C	C	I	A/R		C	C	C	C
Identify and categorise IT resources based on recovery objectives.				C		A/R		C	I	C	I
Define and execute change control procedures to ensure that the IT continuity plan is current.				I		A/R		R	R	R	I
Regularly test the IT continuity plan.				I	I	A/R		C	C	I	I
Develop a follow-on action plan from test results.				C	I	A/R	C	R	R	R	I
Plan and conduct IT continuity training.				I	R	A/R		C	R	I	I
Plan IT services recovery and resumption.		I	I	C	C	A/R	C	R	R	R	C
Plan and implement backup storage and protection.				I		A/R		C	C	I	I
Establish procedures for conducting post-resumption reviews.				C	I	A/R		C	C		C

A **RACI** chart identifies who is **R**esponsible, **A**ccountable, **C**onsulted and/or **I**nformed.

Goals and Metrics



IT

Goals:
- Make sure that IT services are available as required.
- Ensure minimal business impact in the event of an IT service disruption or change.
- Ensure that IT services and infrastructure can resist and recover from failures due to error, deliberate attack or disaster.

Metrics:
- Number of hours lost per user per month due to unplanned outages

Process

Goals:
- Establish an IT continuity plan that supports business continuity plans.
- Develop IT continuity plans that can be executed and are tested and maintained.
- Minimise the probability of IT service interruption.

Metrics:
- Percent of availability SLAs met
- Number of business-critical processes relying on IT not covered by IT continuity plan
- Percent of tests that achieve recovery objectives
- Frequency of service interruption of critical systems

Activities

Goals:
- Developing and maintaining (improving) IT contingency plans
- Training on and testing IT contingency plans
- Storing copies of contingency plans and data at offsite locations

Metrics:
- Elapsed time between tests of any given element of IT continuity plan
- Number of IT continuity training hours per year per relevant IT employee
- Percent of critical infrastructure components with automated availability monitoring
- Frequency of review of IT continuity plan

Maturity Model

DS4 Ensure Continuous Service

Management of the process of *Ensure continuous service* that satisfies the business requirement for IT of *ensuring minimal business impact in the event of an IT service interruption* is:

0 Non-existent when
There is no understanding of the risks, vulnerabilities and threats to IT operations or the impact of loss of IT services to the business. Service continuity is not considered to need management attention.

1 Initial/*Ad Hoc* when
Responsibilities for continuous service are informal, and the authority to execute responsibilities is limited. Management is becoming aware of the risks related to and the need for continuous service. The focus of management attention on continuous service is on infrastructure resources, rather than on the IT services. Users implement workarounds in response to disruptions of services. The response of IT to major disruptions is reactive and unprepared. Planned outages are scheduled to meet IT needs but do not consider business requirements.

2 Repeatable but Intuitive when
Responsibility for ensuring continuous service is assigned. The approaches to ensuring continuous service are fragmented. Reporting on system availability is sporadic, may be incomplete and does not take business impact into account. There is no documented IT continuity plan, although there is commitment to continuous service availability and its major principles are known. An inventory of critical systems and components exists, but it may not be reliable. Continuous service practices are emerging, but success relies on individuals.

3 Defined when
Accountability for the management of continuous service is unambiguous. Responsibilities for continuous service planning and testing are clearly defined and assigned. The IT continuity plan is documented and based on system criticality and business impact. There is periodic reporting of continuous service testing. Individuals take the initiative for following standards and receiving training to deal with major incidents or a disaster. Management communicates consistently the need to plan for ensuring continuous service. High-availability components and system redundancy are being applied. An inventory of critical systems and components is maintained.

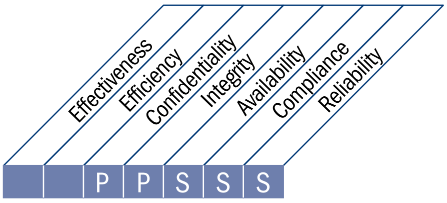
4 Managed and Measurable when
Responsibilities and standards for continuous service are enforced. The responsibility to maintain the continuous service plan is assigned. Maintenance activities are based on the results of continuous service testing, internal good practices, and the changing IT and business environment. Structured data about continuous service are being gathered, analysed, reported and acted upon. Formal and mandatory training is provided on continuous service processes. System availability good practices are being consistently deployed. Availability practices and continuous service planning influence each other. Discontinuity incidents are classified, and the increasing escalation path for each is well known to all involved. Goals and metrics for continuous service have been developed and agreed upon but may be inconsistently measured.

5 Optimised when
Integrated continuous service processes take into account benchmarking and best external practices. The IT continuity plan is integrated with the business continuity plans and is routinely maintained. The requirement for ensuring continuous service is secured from vendors and major suppliers. Global testing of the IT continuity plan occurs, and test results are input for updating the plan. The gathering and analysis of data are used for continuous improvement of the process. Availability practices and continuous service planning are fully aligned. Management ensures that a disaster or major incident will not occur as a result of a single point of failure. Escalation practices are understood and thoroughly enforced. Goals and metrics on continuous service achievement are measured in a systematic fashion. Management adjusts the planning for continuous service in response to the measures.

Process Description

DS5 Ensure Systems Security

The need to maintain the integrity of information and protect IT assets requires a security management process. This process includes establishing and maintaining IT security roles and responsibilties, policies, standards, and procedures. Security management also includes performing security monitoring and periodic testing and implementing corrective actions for identified security weaknesses or incidents. Effective security management protects all IT assets to minimise the business impact of security vulnerabilities and incidents.



Plan and Organise
Acquire and Implement
Deliver and Support
Monitor and Evaluate

Control over the IT process of

Ensure systems security

that satisfies the business requirement for IT of

maintaining the integrity of information and processing infrastructure and minimising the impact of security vulnerabilities and incidents

by focusing on

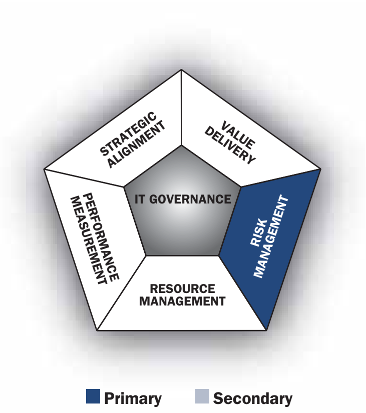
defining IT security policies, plans and procedures, and monitoring, detecting, reporting and resolving security vulnerabilities and incidents

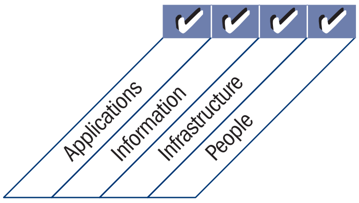
is achieved by

- Understanding security requirements, vulnerabilities and threats
- Managing user identities and authorisations in a standardised manner
- Testing security regularly

and is measured by

- Number of incidents damaging the organisation's reputation with the public
- Number of systems where security requirements are not met
- Number of violations in segregation of duties





Control Objectives

DS5 Ensure Systems Security

DS5.1 Management of IT Security

Manage IT security at the highest appropriate organisational level, so the management of security actions is in line with business requirements.

DS5.2 IT Security Plan

Translate business, risk and compliance requirements into an overall IT security plan, taking into consideration the IT infrastructure and the security culture. Ensure that the plan is implemented in security policies and procedures together with appropriate investments in services, personnel, software and hardware. Communicate security policies and procedures to stakeholders and users.

DS5.3 Identity Management

Ensure that all users (internal, external and temporary) and their activity on IT systems (business application, IT environment, system operations, development and maintenance) are uniquely identifiable. Enable user identities via authentication mechanisms. Confirm that user access rights to systems and data are in line with defined and documented business needs and that job requirements are attached to user identities. Ensure that user access rights are requested by user management, approved by system owners and implemented by the security-responsible person. Maintain user identities and access rights in a central repository. Deploy cost-effective technical and procedural measures, and keep them current to establish user identification, implement authentication and enforce access rights.

DS5.4 User Account Management

Address requesting, establishing, issuing, suspending, modifying and closing user accounts and related user privileges with a set of user account management procedures. Include an approval procedure outlining the data or system owner granting the access privileges. These procedures should apply for all users, including administrators (privileged users) and internal and external users, for normal and emergency cases. Rights and obligations relative to access to enterprise systems and information should be contractually arranged for all types of users. Perform regular management review of all accounts and related privileges.

DS5.5 Security Testing, Surveillance and Monitoring

Test and monitor the IT security implementation in a proactive way. IT security should be reaccredited in a timely manner to ensure that the approved enterprise's information security baseline is maintained. A logging and monitoring function will enable the early prevention and/or detection and subsequent timely reporting of unusual and/or abnormal activities that may need to be addressed.

DS5.6 Security Incident Definition

Clearly define and communicate the characteristics of potential security incidents so they can be properly classified and treated by the incident and problem management process.

DS5.7 Protection of Security Technology

Make security-related technology resistant to tampering, and do not disclose security documentation unnecessarily.

DS5.8 Cryptographic Key Management

Determine that policies and procedures are in place to organise the generation, change, revocation, destruction, distribution, certification, storage, entry, use and archiving of cryptographic keys to ensure the protection of keys against modification and unauthorised disclosure.

DS5.9 Malicious Software Prevention, Detection and Correction

Put preventive, detective and corrective measures in place (especially up-to-date security patches and virus control) across the organisation to protect information systems and technology from malware (e.g., viruses, worms, spyware, spam).

DS5.10 Network Security

Use security techniques and related management procedures (e.g., firewalls, security appliances, network segmentation, intrusion detection) to authorise access and control information flows from and to networks.

DS5.11 Exchange of Sensitive Data

Exchange sensitive transaction data only over a trusted path or medium with controls to provide authenticity of content, proof of submission, proof of receipt and non-repudiation of origin.

Management Guidelines

DS5 Ensure Systems Security

From	Inputs
PO2	Information architecture; assigned data classifications
PO3	Technology standards
PO9	Risk assessment
AI2	Application security controls specification
DS1	OLAs

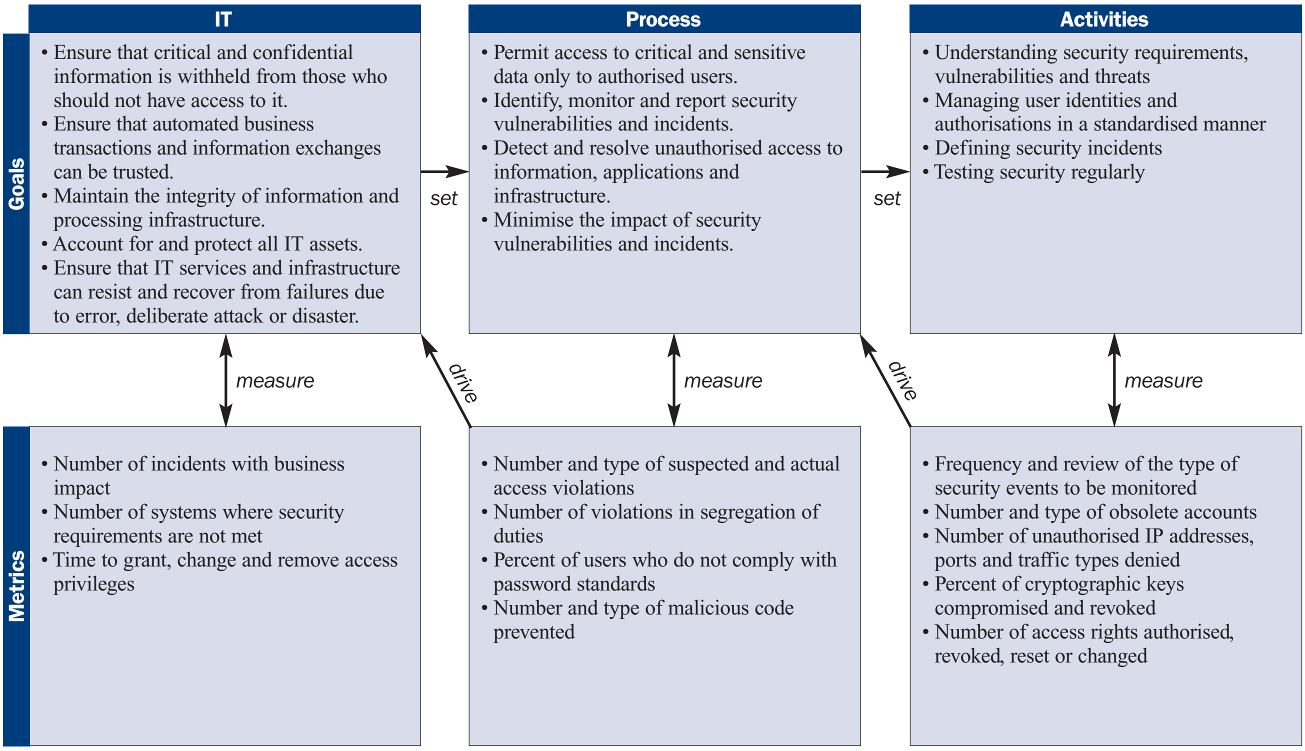
Outputs	To						
Security incident definition	DS8						
Specific training requirements on security awareness	DS7						
Process performance reports	ME1						
Required security changes	AI6						
Security threats and vulnerabilities	PO9						
IT security plan and policies	DS11						

RACI Chart

Activities \ Functions	CEO	CFO	Business Executive	CIO	Business Process Owner	Head Operations	Chief Architect	Head Development	Head IT Administration	PMO	Compliance, Audit, Risk and Security
Define and maintain an IT security plan.	I	C	C	A	C	C	C	C	I	I	R
Define, establish and operate an identity (account) management process.			I	A	C	R	R	I			C
Monitor potential and actual security incidents.				A	I	R	C	C			R
Periodically review and validate user access rights and privileges.				I	A	C					R
Establish and maintain procedures for maintaining and safeguarding cryptographic keys.				A		R			I		C
Implement and maintain technical and procedural controls to protect information flows across networks.				A	C	C	R	R			C
Conduct regular vulnerability assessments.		I		A	I	C	C	C			R

A **RACI** chart identifies who is **R**esponsible, **A**ccountable, **C**onsulted and/or **I**nformed.

Goals and Metrics



IT

Goals:
- Ensure that critical and confidential information is withheld from those who should not have access to it.
- Ensure that automated business transactions and information exchanges can be trusted.
- Maintain the integrity of information and processing infrastructure.
- Account for and protect all IT assets.
- Ensure that IT services and infrastructure can resist and recover from failures due to error, deliberate attack or disaster.

Metrics:
- Number of incidents with business impact
- Number of systems where security requirements are not met
- Time to grant, change and remove access privileges

Process

Goals:
- Permit access to critical and sensitive data only to authorised users.
- Identify, monitor and report security vulnerabilities and incidents.
- Detect and resolve unauthorised access to information, applications and infrastructure.
- Minimise the impact of security vulnerabilities and incidents.

Metrics:
- Number and type of suspected and actual access violations
- Number of violations in segregation of duties
- Percent of users who do not comply with password standards
- Number and type of malicious code prevented

Activities

Goals:
- Understanding security requirements, vulnerabilities and threats
- Managing user identities and authorisations in a standardised manner
- Defining security incidents
- Testing security regularly

Metrics:
- Frequency and review of the type of security events to be monitored
- Number and type of obsolete accounts
- Number of unauthorised IP addresses, ports and traffic types denied
- Percent of cryptographic keys compromised and revoked
- Number of access rights authorised, revoked, reset or changed

Maturity Model

DS5 Ensure Systems Security

Management of the process of *Ensure systems security* that satisfies the business requirements for IT of *maintaining the integrity of information and processing infrastructure and minimising the impact of security vulnerabilities and incidents* is:

0 Non-existent when
The organisation does not recognise the need for IT security. Responsibilities and accountabilities are not assigned for ensuring security. Measures supporting the management of IT security are not implemented. There is no IT security reporting and no response process for IT security breaches. There is a complete lack of a recognisable system security administration process.

1 Initial/*Ad Hoc* when
The organisation recognises the need for IT security. Awareness of the need for security depends primarily on the individual. IT security is addressed on a reactive basis. IT security is not measured. Detected IT security breaches invoke finger-pointing responses, because responsibilities are unclear. Responses to IT security breaches are unpredictable.

2 Repeatable but Intuitive when
Responsibilities and accountabilities for IT security are assigned to an IT security co-ordinator, although the management authority of the co-ordinator is limited. Awareness of the need for security is fragmented and limited. Although security-relevant information is produced by systems, it is not analysed. Services from third parties may not address the specific security needs of the organisation. Security policies are being developed, but skills and tools are inadequate. IT security reporting is incomplete, misleading or not pertinent. Security training is available but is undertaken primarily at the initiative of the individual. IT security is seen primarily as the responsibility and domain of IT and the business does not see IT security as within its domain.

3 Defined when
Security awareness exists and is promoted by management. IT security procedures are defined and aligned with IT security policy. Responsibilities for IT security are assigned and understood, but not consistently enforced. An IT security plan and security solutions exist as driven by risk analysis. Reporting on security does not contain a clear business focus. *Ad hoc* security testing (e.g., intrusion testing) is performed. Security training is available for IT and the business, but is only informally scheduled and managed.

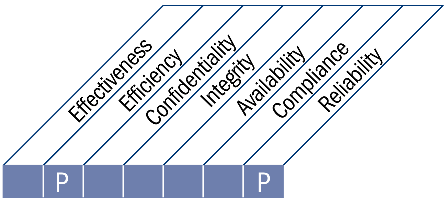
4 Managed and Measurable when
Responsibilities for IT security are clearly assigned, managed and enforced. IT security risk and impact analysis is consistently performed. Security policies and procedures are completed with specific security baselines. Exposure to methods for promoting security awareness is mandatory. User identification, authentication and authorisation are standardised. Security certification is pursued for staff members who are responsible for the audit and management of security. Security testing is completed using standard and formalised processes, leading to improvements of security levels. IT security processes are co-ordinated with an overall organisation security function. IT security reporting is linked to business objectives. IT security training is conducted in both the business and IT. IT security training is planned and managed in a manner that responds to business needs and defined security risk profiles. Goals and metrics for security management have been defined but are not yet measured.

5 Optimised when
IT security is a joint responsibility of business and IT management and is integrated with corporate security business objectives. IT security requirements are clearly defined, optimised and included in an approved security plan. Users and customers are increasingly accountable for defining security requirements, and security functions are integrated with applications at the design stage. Security incidents are promptly addressed with formalised incident response procedures supported by automated tools. Periodic security assessments are conducted to evaluate the effectiveness of the implementation of the security plan. Information on threats and vulnerabilities is systematically collected and analysed. Adequate controls to mitigate risks are promptly communicated and implemented. Security testing, root cause analysis of security incidents and proactive identification of risk are used for continuous process improvements. Security processes and technologies are integrated organisationwide. Metrics for security management are measured, collected and communicated. Management uses these measures to adjust the security plan in a continuous improvement process.

Process Description

DS6 Identify and Allocate Costs

The need for a fair and equitable system of allocating IT costs to the business requires accurate measurement of IT costs and agreement with business users on fair allocation. This process includes building and operating a system to capture, allocate and report IT costs to the users of services. A fair system of allocation enables the business to make more informed decisions regarding the use of IT services.



Control over the IT process of

Identify and allocate costs

that satisfies the business requirement for IT of

ensuring transparency and understanding of IT costs and improving cost-efficiency through well-informed use of IT services

by focusing on

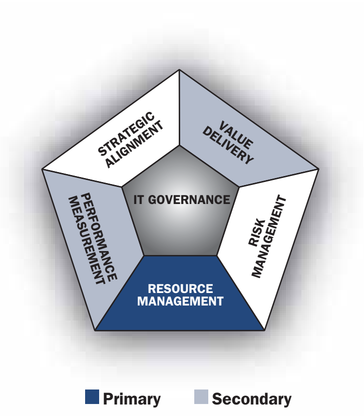
complete and accurate capture of IT costs, a fair system of allocation agreed upon by business users, and a system for timely reporting of IT use and costs allocated

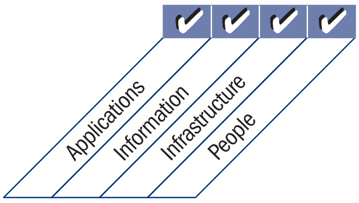
is achieved by

- Aligning charges to the quality and quantity of services provided
- Building and agreeing on a complete cost model
- Implementing charges as per the agreed-upon policy

and is measured by

- Percent of IT service bills accepted/paid by business management
- Percent of variance amongst budgets, forecasts and actual costs
- Percent of overall IT costs that are allocated according to the agreed-upon cost models





Control Objectives

DS6 Identify and Allocate Costs

DS6.1 Definition of Services
Identify all IT costs, and map them to IT services to support a transparent cost model. IT services should be linked to business processes such that the business can identify associated service billing levels.

DS6.2 IT Accounting
Capture and allocate actual costs according to the enterprise cost model. Variances between forecasts and actual costs should be analysed and reported on, in compliance with the enterprise's financial measurement systems.

DS6.3 Cost Modelling and Charging
Establish and use an IT costing model based on the service definitions that support the calculation of chargeback rates per service. The IT cost model should ensure that charging for services is identifiable, measurable and predictable by users to encourage proper use of resources.

DS6.4 Cost Model Maintenance
Regularly review and benchmark the appropriateness of the cost/recharge model to maintain its relevance and appropriateness to the evolving business and IT activities.

Management Guidelines

DS6 Identify and Allocate Costs

From	Inputs
PO4	Documented system owners
PO5	Cost-benefit reports, IT budgets
PO10	Detailed project plans
DS1	SLAs and OLAs

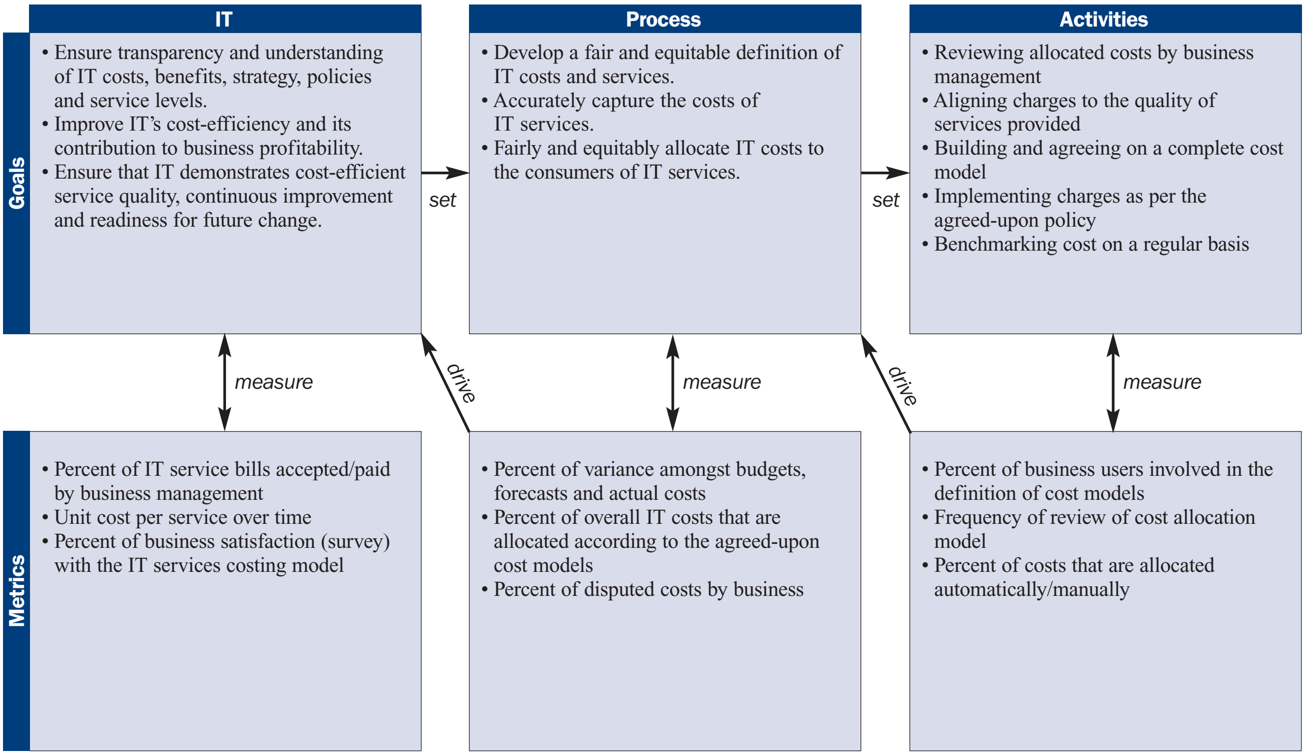
Outputs	To						
IT financials	PO5						
Process performance reports	ME1						

RACI Chart

Activities	CEO	CFO	Business Executive	CIO	Business Process Owner	Head Operations	Chief Architect	Head Development	Head IT Administration	PMO	Compliance, Audit, Risk and Security
Map the IT infrastructure to services provided/business processes supported.		C	C	A	C	C	C	C	R	C	
Identify all IT costs (e.g., people, technology) and map them to IT services on a unit cost basis.		C		A		C	C	C	R	C	
Establish and maintain an IT accounting and cost control process.		C	C	A	C	C	C	C	R	C	
Establish and maintain charging policies and procedures.		C	C	A	C	C	C	C	R	C	

A **RACI** chart identifies who is **R**esponsible, **A**ccountable, **C**onsulted and/or **I**nformed.

Goals and Metrics



IT

Goals:

- Ensure transparency and understanding of IT costs, benefits, strategy, policies and service levels.
- Improve IT's cost-efficiency and its contribution to business profitability.
- Ensure that IT demonstrates cost-efficient service quality, continuous improvement and readiness for future change.

Metrics:

- Percent of IT service bills accepted/paid by business management
- Unit cost per service over time
- Percent of business satisfaction (survey) with the IT services costing model

Process

Goals:

- Develop a fair and equitable definition of IT costs and services.
- Accurately capture the costs of IT services.
- Fairly and equitably allocate IT costs to the consumers of IT services.

Metrics:

- Percent of variance amongst budgets, forecasts and actual costs
- Percent of overall IT costs that are allocated according to the agreed-upon cost models
- Percent of disputed costs by business

Activities

Goals:

- Reviewing allocated costs by business management
- Aligning charges to the quality of services provided
- Building and agreeing on a complete cost model
- Implementing charges as per the agreed-upon policy
- Benchmarking cost on a regular basis

Metrics:

- Percent of business users involved in the definition of cost models
- Frequency of review of cost allocation model
- Percent of costs that are allocated automatically/manually

Maturity Model

DS6 Identify and Allocate Costs

Management of the process of *Identify and allocate* costs that satisfies the business requirement for IT of *ensuring transparency and understanding of IT costs and improving cost-efficiency through well-informed use of IT services* is:

0 Non-existent when
There is a complete lack of any recognisable process for identifying and allocating costs with respect to information services provided. The organisation does not even recognise that there is an issue to be addressed with respect to cost accounting, and there is no communication about the issue.

1 Initial/*Ad Hoc* when
There is a general understanding of the overall costs for information services, but there is no breakdown of costs per user, customer, department, groups of users, service functions, projects or deliverables. There is virtually no cost monitoring, with only aggregate cost reporting to management. IT costs are allocated as an operational overhead. Business is provided with no information on the cost or benefits of service provision.

2 Repeatable but Intuitive when
There is overall awareness of the need to identify and allocate costs. Cost allocation is based on informal or rudimentary cost assumptions, e.g., hardware costs, and there is virtually no linking to value drivers. Cost allocation processes are repeatable. There is no formal training or communication on standard cost identification and allocation procedures. Responsibility for the collection or allocation of costs is not assigned.

3 Defined when
There is a defined and documented information services cost model. A process for relating IT costs to the services provided to users is defined. An appropriate level of awareness exists regarding the costs attributable to information services. The business is provided with rudimentary information on costs.

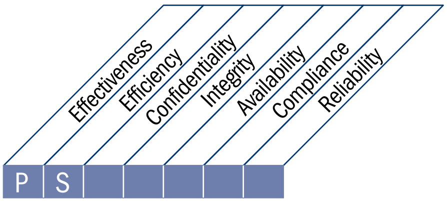
4 Managed and Measurable when
Information services cost management responsibilities and accountabilities are defined and fully understood at all levels and are supported by formal training. Direct and indirect costs are identified and reported in a timely and automated manner to management, business process owners and users. Generally, there is cost monitoring and evaluation, and actions are taken if cost deviations are detected. Information services cost reporting is linked to business objectives and SLAs and is monitored by business process owners. A finance function reviews the reasonableness of the cost allocation process. An automated cost accounting system exists, but is focused on the information services function rather than on business processes. Goals and metrics are agreed to for cost measurement but are inconsistently measured.

5 Optimised when
Costs of services provided are identified, captured, summarised and reported to management, business process owners and users. Costs are identified as chargeable items and could support a chargeback system that appropriately bills users for services provided, based on utilisation. Cost details support SLAs. The monitoring and evaluation of costs of services are used to optimise the cost of IT resources. Cost figures obtained are used to verify benefit realisation in the organisation's budgeting process. Information services cost reporting provides early warning of changing business requirements through intelligent reporting systems. A variable cost model is utilised, derived from volumes processed for each service provided. Cost management is refined to a level of industry practice, based on the result of continuous improvement and benchmarking with other organisations. Cost optimisation is an ongoing process. Management reviews goals and metrics as part of a continuous improvement process in redesigning cost measurement systems.

Process Description

DS7 Educate and Train Users

Effective education of all users of IT systems, including those within IT, requires identifying the training needs of each user group. In addition to identifying needs, this process includes defining and executing a strategy for effective training and measuring the results. An effective training programme increases effective use of technology by reducing user errors, increasing productivity and increasing compliance with key controls, such as user security measures.



Plan and Organise
Acquire and Implement
Deliver and Support
Monitor and Evaluate

Control over the IT process of

Educate and train users

that satisfies the business requirement for IT of

effectively and efficiently using applications and technology solutions and ensuring user compliance with policies and procedures

by focusing on

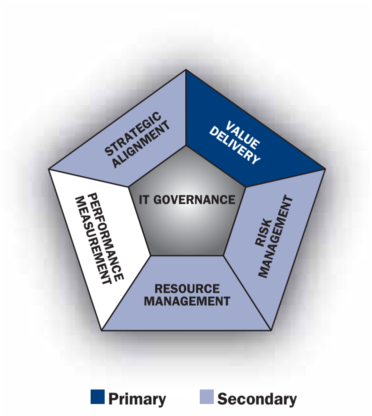
a clear understanding of IT user training needs, execution of an effective training strategy and measurement of the results

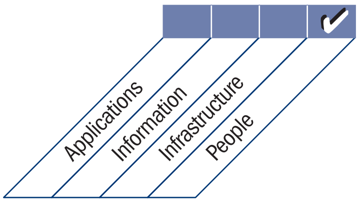
is achieved by

- Establishing training curricula
- Organising training
- Delivering training
- Monitoring and reporting on training effectiveness

and is measured by

- Number of service desk calls due to lack of user training
- Percent of stakeholder satisfaction with training provided
- Time lag between identification of a training need and the delivery of the training





Control Objectives

DS7 Educate and Train Users

DS7.1 Identification of Education and Training Needs

Establish and regularly update a curriculum for each target group of employees considering:
- Current and future business needs and strategy
- Value of information as an asset
- Corporate values (ethical values, control and security culture, etc.)
- Implementation of new IT infrastructure and software (i.e., packages, applications)
- Current and future skills, competence profiles, and certification and/or credentialing needs as well as required reaccreditation
- Delivery methods (e.g., classroom, web-based), target group size, accessibility and timing

DS7.2 Delivery of Training and Education

Based on the identified education and training needs, identify target groups and their members, efficient delivery mechanisms, teachers, trainers, and mentors. Appoint trainers and organise timely training sessions. Record registration (including prerequisites), attendance and training session performance evaluations.

DS7.3 Evaluation of Training Received

Evaluate education and training content delivery upon completion for relevance, quality, effectiveness, the retention of knowledge, cost and value. The results of this evaluation should serve as input for future curriculum definition and the delivery of training sessions.

Management Guidelines

DS7 Educate and Train Users

From	Inputs
PO7	Users' skills and competencies, including individual training; specific training requirements
AI4	Training materials, knowledge transfer requirements for solutions implementation
DS1	OLAs
DS5	Specific training requirements on security awareness
DS8	User satisfaction reports

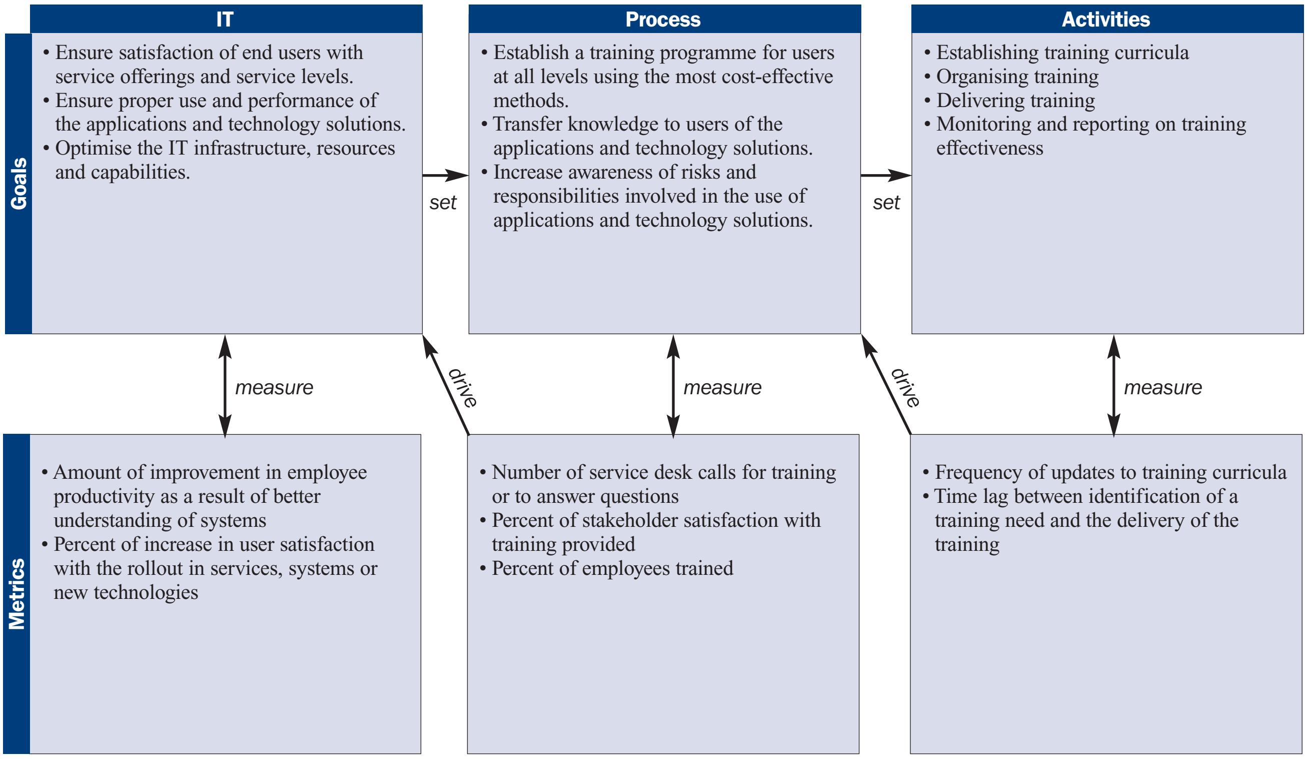
Outputs	To
Process performance reports	ME1
Required documentation updates	AI4

RACI Chart

Activities	CEO	CFO	Business Executive	CIO	Business Process Owner	Head Operations	Chief Architect	Head Development	Head IT Administration	PMO	Compliance, Audit, Risk and Security	Training Department
Identify and characterise users' training needs.			C	A	R	C	C	C	C	C	C	R
Build a training programme.			C	A	R	C	I	C	C	C	I	R
Conduct awareness, education and training activities.			I	A	C	C	I	C	C	C	I	R
Perform training evaluation.			I	A	R	C	I	C	C	C	I	R
Identify and evaluate best training delivery methods and tools.			I	A/R	R	C	C	C	C	C	C	R

A **RACI** chart identifies who is **R**esponsible, **A**ccountable, **C**onsulted and/or **I**nformed.

Goals and Metrics



Goals

IT
- Ensure satisfaction of end users with service offerings and service levels.
- Ensure proper use and performance of the applications and technology solutions.
- Optimise the IT infrastructure, resources and capabilities.

Process
- Establish a training programme for users at all levels using the most cost-effective methods.
- Transfer knowledge to users of the applications and technology solutions.
- Increase awareness of risks and responsibilities involved in the use of applications and technology solutions.

Activities
- Establishing training curricula
- Organising training
- Delivering training
- Monitoring and reporting on training effectiveness

Metrics

- Amount of improvement in employee productivity as a result of better understanding of systems
- Percent of increase in user satisfaction with the rollout in services, systems or new technologies

- Number of service desk calls for training or to answer questions
- Percent of stakeholder satisfaction with training provided
- Percent of employees trained

- Frequency of updates to training curricula
- Time lag between identification of a training need and the delivery of the training

Maturity Model

DS7 Educate and Train Users

Management of the process of *Educate and train users* that satisfies the business requirement for IT of *effectively and efficiently using applications and technology solutions and ensuring user compliance with policies and procedures* is:

0 Non-existent when
There is a complete lack of a training and education programme. The organisation does not even recognise that there is an issue to be addressed with respect to training, and there is no communication on the issue.

1 Initial/*Ad Hoc* when
There is evidence that the organisation has recognised the need for a training and education programme, but there are no standardised processes. In the absence of an organised programme, employees identify and attend training courses on their own. Some of these training courses address the issues of ethical conduct, system security awareness and security practices. The overall management approach lacks any cohesion, and there is only sporadic and inconsistent communication on issues and approaches to address training and education.

2 Repeatable but Intuitive when
There is awareness of the need for a training and education programme and for associated processes throughout the organisation. Training is beginning to be identified in the individual performance plans of employees. Processes are developed to the stage where informal training and education classes are taught by different instructors, whilst covering the same subject matter with different approaches. Some of the classes address the issues of ethical conduct and system security awareness and practices. There is high reliance on the knowledge of individuals. However, there is consistent communication on the overall issues and the need to address them.

3 Defined when
A training and education programme is instituted and communicated, and employees and managers identify and document training needs. Training and education processes are standardised and documented. Budgets, resources, facilities and trainers are being established to support the training and education programme. Formal classes are given to employees on ethical conduct and system security awareness and practices. Most training and education processes are monitored, but not all deviations are likely to be detected by management. Analysis of training and education problems is only occasionally applied.

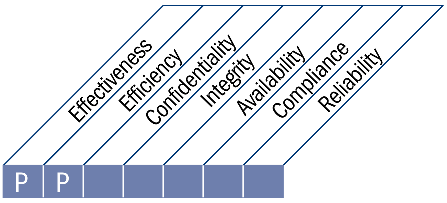
4 Managed and Measurable when
There is a comprehensive training and education programme that yields measurable results. Responsibilities are clear, and process ownership is established. Training and education are components of employee career paths. Management supports and attends training and educational sessions. All employees receive ethical conduct and system security awareness training. All employees receive the appropriate level of system security practices training in protecting against harm from failures affecting availability, confidentiality and integrity. Management monitors compliance by constantly reviewing and updating the training and education programme and processes. Processes are under improvement and enforce best internal practices.

5 Optimised when
Training and education result in an improvement of individual performance. Training and education are critical components of the employee career paths. Sufficient budgets, resources, facilities and instructors are provided for the training and education programmes. Processes are refined and are under continuous improvement, taking advantage of best external practices and maturity modelling with benchmarking against other organisations. All problems and deviations are analysed for root causes, and efficient action is expediently identified and taken. There is a positive attitude with respect to ethical conduct and system security principles. IT is used in an extensive, integrated and optimised manner to automate and provide tools for the training and education programme. External training experts are leveraged, and benchmarks are used for guidance.

Process Description

DS8 Manage Service Desk and Incidents

Timely and effective response to IT user queries and problems requires a well-designed and well-executed service desk and incident management process. This process includes setting up a service desk function with registration, incident escalation, trend and root cause analysis, and resolution. The business benefits include increased productivity through quick resolution of user queries. In addition, the business can address root causes (such as poor user training) through effective reporting.



Control over the IT process of

Manage service desk and incidents

that satisfies the business requirement for IT of

enabling effective use of IT systems by ensuring resolution and analysis of end-user queries, questions and incidents

by focusing on

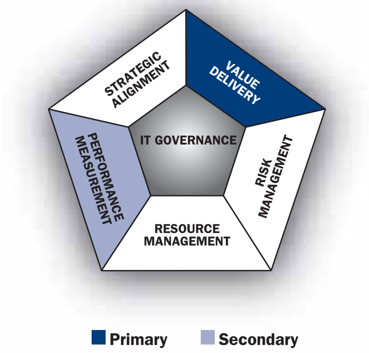
a professional service desk function with quick response, clear escalation procedures, and resolution and trend analysis

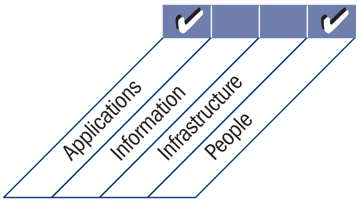
is achieved by

- Installing and operating a service desk
- Monitoring and reporting trends
- Defining clear escalation criteria and procedures

and is measured by

- Amount of user satisfaction with first-line support
- Percent of incidents resolved within agreed-upon/acceptable period of time
- Call abandonment rate





Control Objectives

DS8 Manage Service Desk and Incidents

DS8.1 Service Desk

Establish a service desk function, which is the user interface with IT, to register, communicate, dispatch and analyse all calls, reported incidents, service requests and information demands. There should be monitoring and escalation procedures based on agreed-upon service levels relative to the appropriate SLA that allow classification and prioritisation of any reported issue as an incident, service request or information request. Measure end users' satisfaction with the quality of the service desk and IT services.

DS8.2 Registration of Customer Queries

Establish a function and system to allow logging and tracking of calls, incidents, service requests and information needs. It should work closely with such processes as incident management, problem management, change management, capacity management and availability management. Incidents should be classified according to a business and service priority and routed to the appropriate problem management team, where necessary. Customers should be kept informed of the status of their queries.

DS8.3 Incident Escalation

Establish service desk procedures, so incidents that cannot be resolved immediately are appropriately escalated according to limits defined in the SLA and, if appropriate, workarounds are provided. Ensure that incident ownership and life cycle monitoring remain with the service desk for user-based incidents, regardless which IT group is working on resolution activities.

DS8.4 Incident Closure

Establish procedures for the timely monitoring of clearance of customer queries. When the incident has been resolved, ensure that the service desk records the resolution steps, and confirm that the action taken has been agreed to by the customer. Also record and report unresolved incidents (known errors and workarounds) to provide information for proper problem management.

DS8.5 Reporting and Trend Analysis

Produce reports of service desk activity to enable management to measure service performance and service response times and to identify trends or recurring problems, so service can be continually improved.

Management Guidelines

DS8 Manage Service Desk and Incidents

From	Inputs
AI4	User, operational, support, technical and administration manuals
AI6	Change authorisation
AI7	Released configuration items
DS1	SLAs and OLAs
DS4	Incident/disaster thresholds
DS5	Security incident definition
DS9	IT configuration/asset details
DS10	Known problems, known errors and workarounds
DS13	Incident tickets

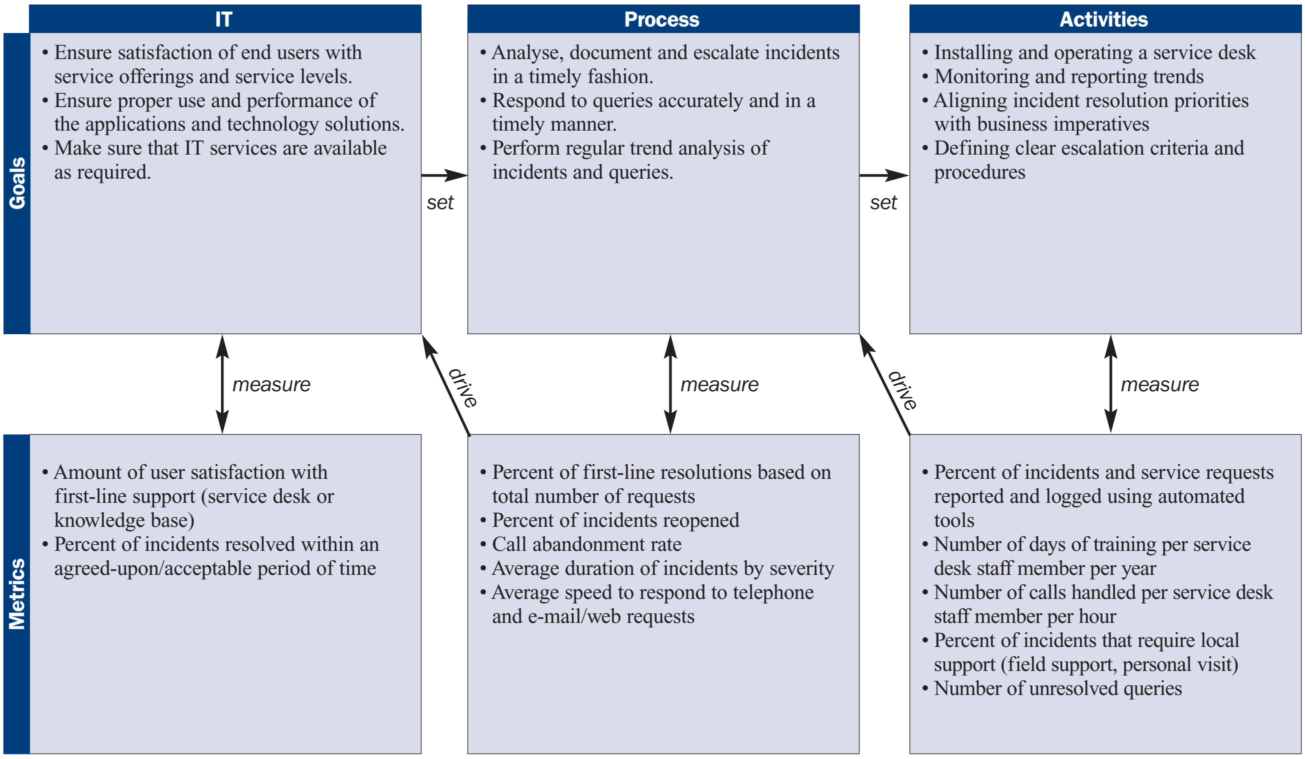
Outputs	To						
Service requests/request for change (RFC)	AI6						
Incident reports	DS10						
Process performance reports	ME1						
User satisfaction reports	DS7	ME1					

RACI Chart

Activities \ Functions	CEO	CFO	Business Executive	CIO	Business Process Owner	Head Operations	Chief Architect	Head Development	Head IT Administration	PMO	Compliance, Audit, Risk and Security	Service Desk/ Incident Manager
Create classification (severity and impact) and escalation procedures (functional and hierarchical).				C	C	C	C	C	C		C	A/R
Detect and record incidents/service requests/information requests.												A/R
Classify, investigate and diagnose queries.				I		C	C	C			I	A/R
Resolve, recover and close incidents.					I	R	R	R			C	A/R
Inform users (e.g., status updates).				I	I							A/R
Produce management reporting.	I			I	I	I			I		I	A/R

A **RACI** chart identifies who is **R**esponsible, **A**ccountable, **C**onsulted and/or **I**nformed.

Goals and Metrics



IT

Goals:
- Ensure satisfaction of end users with service offerings and service levels.
- Ensure proper use and performance of the applications and technology solutions.
- Make sure that IT services are available as required.

Metrics:
- Amount of user satisfaction with first-line support (service desk or knowledge base)
- Percent of incidents resolved within an agreed-upon/acceptable period of time

Process

Goals:
- Analyse, document and escalate incidents in a timely fashion.
- Respond to queries accurately and in a timely manner.
- Perform regular trend analysis of incidents and queries.

Metrics:
- Percent of first-line resolutions based on total number of requests
- Percent of incidents reopened
- Call abandonment rate
- Average duration of incidents by severity
- Average speed to respond to telephone and e-mail/web requests

Activities

Goals:
- Installing and operating a service desk
- Monitoring and reporting trends
- Aligning incident resolution priorities with business imperatives
- Defining clear escalation criteria and procedures

Metrics:
- Percent of incidents and service requests reported and logged using automated tools
- Number of days of training per service desk staff member per year
- Number of calls handled per service desk staff member per hour
- Percent of incidents that require local support (field support, personal visit)
- Number of unresolved queries

Maturity Model

DS8 Manage Service Desk and Incidents

Management of the process of *Manage service desk and incidents* that satisfies the business requirement for IT of *enabling effective use of IT systems by ensuring resolution and analysis of end-user queries, questions and incidents* is:

0 Non-existent when
There is no support to resolve user questions and issues. There is a complete lack of an incident management process. The organisation does not recognise that there is an issue to be addressed.

1 Initial/*Ad Hoc* when
Management recognises that a process supported by tools and personnel is required to respond to user queries and manage incident resolution. There is, however, no standardised process, and only reactive support is provided. Management does not monitor user queries, incidents or trends. There is no escalation process to ensure that problems are resolved.

2 Repeatable but Intuitive when
There is organisational awareness of the need for a service desk function and an incident management process. Assistance is available on an informal basis through a network of knowledgeable individuals. These individuals have some common tools available to assist in incident resolution. There is no formal training and communication on standard procedures, and responsibility is left to the individual.

3 Defined when
The need for a service desk function and incident management process is recognised and accepted. Procedures have been standardised and documented, and informal training is occurring. It is, however, left to the individual to get training and follow the standards. Frequently asked questions (FAQs) and user guidelines are developed, but individuals must find them and may not follow them. Queries and incidents are tracked on a manual basis and individually monitored, but a formal reporting system does not exist. The timely response to queries and incidents is not measured and incidents may go unresolved. Users have received clear communications on where and how to report on problems and incidents.

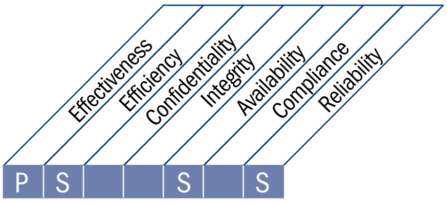
4 Managed and Measurable when
There is a full understanding of the benefits of an incident management process at all levels of the organisation, and the service desk function is established in appropriate organisational units. The tools and techniques are automated with a centralised knowledge base. The service desk staff members closely interact with the problem management staff members. The responsibilities are clear, and effectiveness is monitored. Procedures for communicating, escalating and resolving incidents are established and communicated. Service desk personnel are trained, and processes are improved through the use of task-specific software. Management develops metrics for the performance of the service desk.

5 Optimised when
The incident management process and service desk function are established and well organised and take on a customer service orientation by being knowledgeable, customer-focused and helpful. Metrics are systematically measured and reported. Extensive, comprehensive FAQs are an integral part of the knowledge base. Tools are in place to enable a user to self-diagnose and resolve incidents. Advice is consistent, and incidents are resolved quickly within a structured escalation process. Management utilises an integrated tool for performance statistics of the incident management process and the service desk function. Processes have been refined to the level of best industry practices, based on the results of analysing performance indicators, continuous improvement and benchmarking with other organisations.

Process Description

DS9 Manage the Configuration

Ensuring the integrity of hardware and software configurations requires the establishment and maintenance of an accurate and complete configuration repository. This process includes collecting initial configuration information, establishing baselines, verifying and auditing configuration information, and updating the configuration repository as needed. Effective configuration management facilitates greater system availability, minimises production issues and resolves issues more quickly.



Control over the IT process of

Manage the configuration

that satisfies the business requirement for IT of

optimising the IT infrastructure, resources and capabilities, and accounting for IT assets

by focusing on

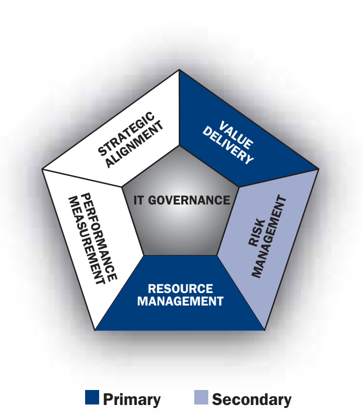
establishing and maintaining an accurate and complete repository of asset configuration attributes and baselines, and comparing them against actual asset configuration

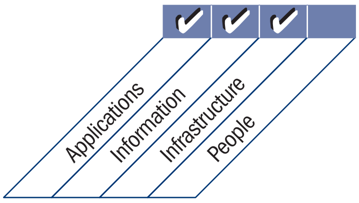
is achieved by

- Establishing a central repository of all configuration items
- Identifying configuration items and maintaining them
- Reviewing integrity of configuration data

and is measured by

- Number of business compliance issues caused by improper configuration of assets
- Number of deviations identified between the configuration repository and actual asset configurations
- Percent of licences purchased and not accounted for in the repository





Control Objectives

DS9 Manage the Configuration

DS9.1 Configuration Repository and Baseline
Establish a supporting tool and a central repository to contain all relevant information on configuration items. Monitor and record all assets and changes to assets. Maintain a baseline of configuration items for every system and service as a checkpoint to which to return after changes..

DS9.2 Identification and Maintenance of Configuration Items
Establish configuration procedures to support management and logging of all changes to the configuration repository. Integrate these procedures with change management, incident management and problem management procedures.

DS9.3 Configuration Integrity Review
Periodically review the configuration data to verify and confirm the integrity of the current and historical configuration. Periodically review installed software against the policy for software usage to identify personal or unlicensed software or any software instances in excess of current license agreements. Report, act on and correct errors and deviations.

Management Guidelines

DS9 Manage the Configuration

From	Inputs
AI4	User, operational, support, technical and administration manuals
AI7	Released configuration items
DS4	Criticality of IT configuration items

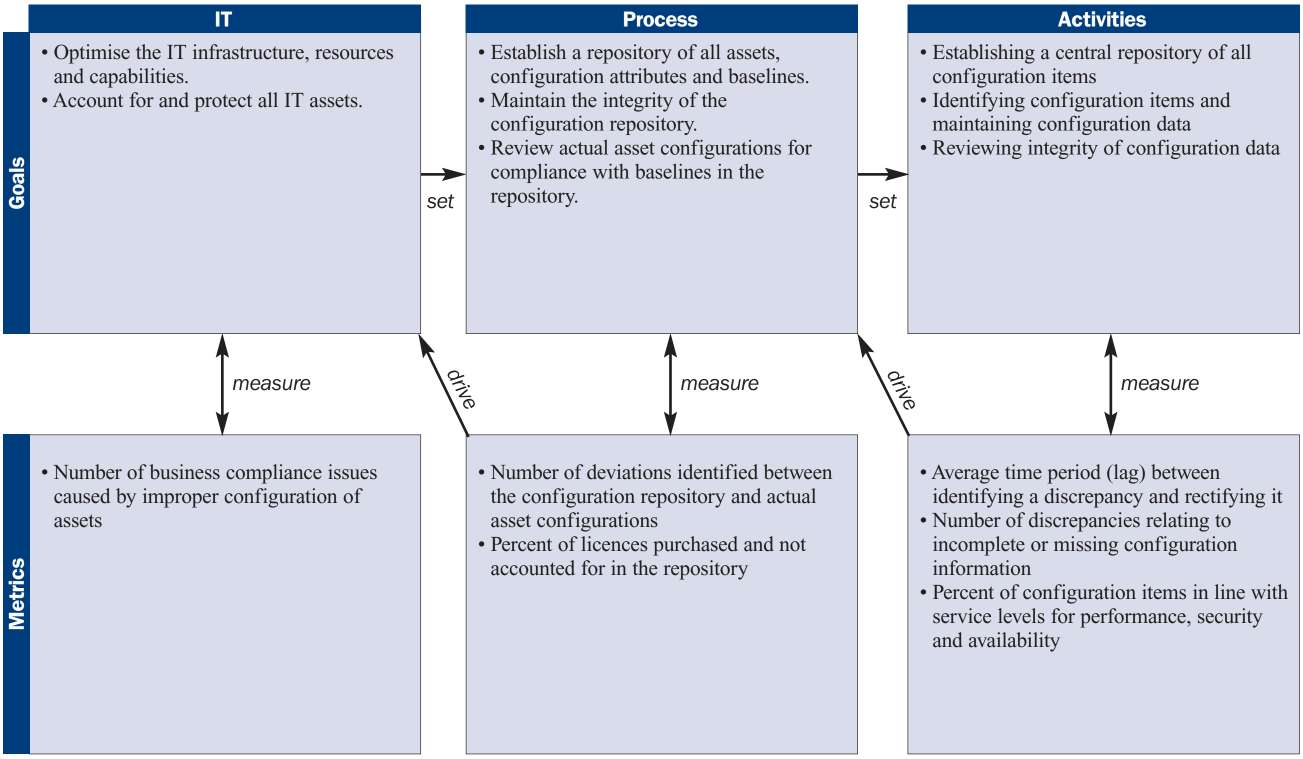
Outputs	To						
IT configuration/asset details	DS8	DS10	DS13				
RFC (where and how to apply the fix)	AI6						
Process performance reports	ME1						

RACI Chart

Activities \ Functions	CEO	CFO	Business Executive	CIO	Business Process Owner	Head Operations	Chief Architect	Head Development	Head IT Administration	PMO	Compliance, Audit, Risk and Security	Configuration Manager
Develop configuration management planning procedures.					C	A	C	I	C		C	R
Collect initial configuration information and establish baselines.						C	C	C			I	A/R
Verify and audit configuration information (includes detection of unauthorised software).		I				A			I		I	A/R
Update configuration repository.						R	R	R			I	A/R

A **RACI** chart identifies who is **R**esponsible, **A**ccountable, **C**onsulted and/or **I**nformed.

Goals and Metrics



IT

Goals:
- Optimise the IT infrastructure, resources and capabilities.
- Account for and protect all IT assets.

Metrics:
- Number of business compliance issues caused by improper configuration of assets

Process

Goals:
- Establish a repository of all assets, configuration attributes and baselines.
- Maintain the integrity of the configuration repository.
- Review actual asset configurations for compliance with baselines in the repository.

Metrics:
- Number of deviations identified between the configuration repository and actual asset configurations
- Percent of licences purchased and not accounted for in the repository

Activities

Goals:
- Establishing a central repository of all configuration items
- Identifying configuration items and maintaining configuration data
- Reviewing integrity of configuration data

Metrics:
- Average time period (lag) between identifying a discrepancy and rectifying it
- Number of discrepancies relating to incomplete or missing configuration information
- Percent of configuration items in line with service levels for performance, security and availability

Maturity Model

DS9 Manage the Configuration

Management of the process of *Manage the configuration* that satisfies the business requirement for IT of *optimising the IT infrastructure, resources and capabilities, and accounting for IT assets* is:

0 Non-existent when
Management does not have an appreciation of the benefits of having a process in place that is capable of reporting on and managing the IT infrastructure, for either hardware or software configurations.

1 Initial/*Ad Hoc* when
The need for configuration management is recognised. Basic configuration management tasks, such as maintaining inventories of hardware and software, are performed on an individual basis. No standard practices are defined.

2 Repeatable but Intuitive when
Management is aware of the need for controlling the IT configuration and understands the benefits of accurate and complete configuration information, but there is implicit reliance on technical personnel knowledge and expertise. Configuration management tools are being employed to a certain degree, but differ amongst platforms. Moreover, no standard working practices are defined. Configuration data content is limited and not used by interrelated processes, such as change management and problem management.

3 Defined when
The procedures and working practices are documented, standardised and communicated, but training and application of the standards is up to the individual. In addition, similar configuration management tools are being implemented across platforms. Deviations from procedures are unlikely to be detected, and physical verifications are performed inconsistently. Some automation occurs to assist in tracking equipment and software changes. Configuration data are being used by interrelated processes.

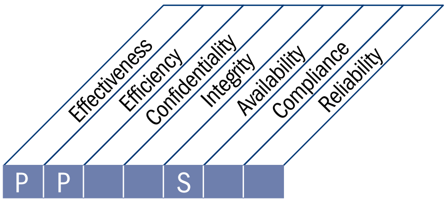
4 Managed and Measurable when
The need to manage the configuration is recognised at all levels of the organisation, and good practices continue to evolve. Procedures and standards are communicated and incorporated into training, and deviations are monitored, tracked and reported. Automated tools, such as push technology, are utilised to enforce standards and improve stability. Configuration management systems do cover most of the IT assets and allow for proper release management and distribution control. Exception analyses, as well as physical verifications, are consistently applied and their root causes are investigated.

5 Optimised when
All IT assets are managed within a central configuration management system that contains all necessary information about components, their interrelationships and events. The configuration data are aligned with vendor catalogues. There is full integration of interrelated processes, and they use and update configuration data in an automated fashion. Baseline audit reports provide essential hardware and software data for repair, service, warranty, upgrade and technical assessments of each individual unit. Rules for limiting installation of unauthorised software are enforced. Management forecasts repairs and upgrades from analysis reports, providing scheduled upgrades and technology refreshment capabilities. Asset tracking and monitoring of individual IT assets protect them and prevent theft, misuse and abuse.

Process Description

DS10 Manage Problems

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



Plan and Organise
Acquire and Implement
Deliver and Support
Monitor and Evaluate

Control over the IT process of

Manage problems

that satisfies the business requirement for IT of

ensuring end users' satisfaction with service offerings and service levels, and reducing solution and service delivery defects and rework

by focusing on

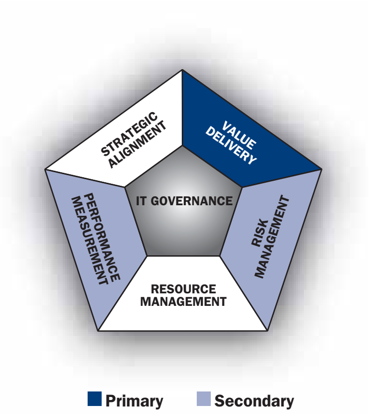
recording, tracking and resolving operational problems; investigating the root cause of all significant problems; and defining solutions for identified operations problems

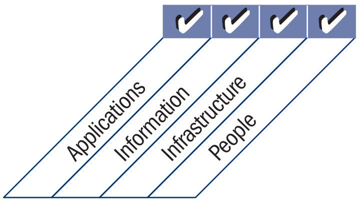
is achieved by

- Performing root cause analysis of reported problems
- Analysing trends
- Taking ownership of problems and progressing problem resolution

and is measured by

- Number of recurring problems with an impact on the business
- Percent of problems resolved within the required time period
- Frequency of reports or updates to an ongoing problem, based on the problem severity





Control Objectives

DS10 Manage Problems

DS10.1 Identification and Classification of Problems

Implement processes to report and classify problems that have been identified as part of incident management. The steps involved in problem classification are similar to the steps in classifying incidents; they are to determine category, impact, urgency and priority. Categorise problems as appropriate into related groups or domains (e.g., hardware, software, support software). These groups may match the organisational responsibilities of the user and customer base, and should be the basis for allocating problems to support staff.

DS10.2 Problem Tracking and Resolution

Ensure that the problem management system provides for adequate audit trail facilities that allow tracking, analysing and determining the root cause of all reported problems considering:

- All associated configuration items
- Outstanding problems and incidents
- Known and suspected errors
- Tracking of problem trends

Identify and initiate sustainable solutions addressing the root cause, raising change requests via the established change management process. Throughout the resolution process, problem management should obtain regular reports from change management on progress in resolving problems and errors. Problem management should monitor the continuing impact of problems and known errors on user services. In the event that this impact becomes severe, problem management should escalate the problem, perhaps referring it to an appropriate board to increase the priority of the (RFC or to implement an urgent change as appropriate. Monitor the progress of problem resolution against SLAs.

DS10.3 Problem Closure

Put in place a procedure to close problem records either after confirmation of successful elimination of the known error or after agreement with the business on how to alternatively handle the problem.

DS10.4 Integration of Configuration, Incident and Problem Management

Integrate the related processes of configuration, incident and problem management to ensure effective management of problems and enable improvements.

Management Guidelines

DS10 Manage Problems

From	Inputs
AI6	Change authorisation
DS8	Incident reports
DS9	IT configuration/asset details
DS13	Error logs

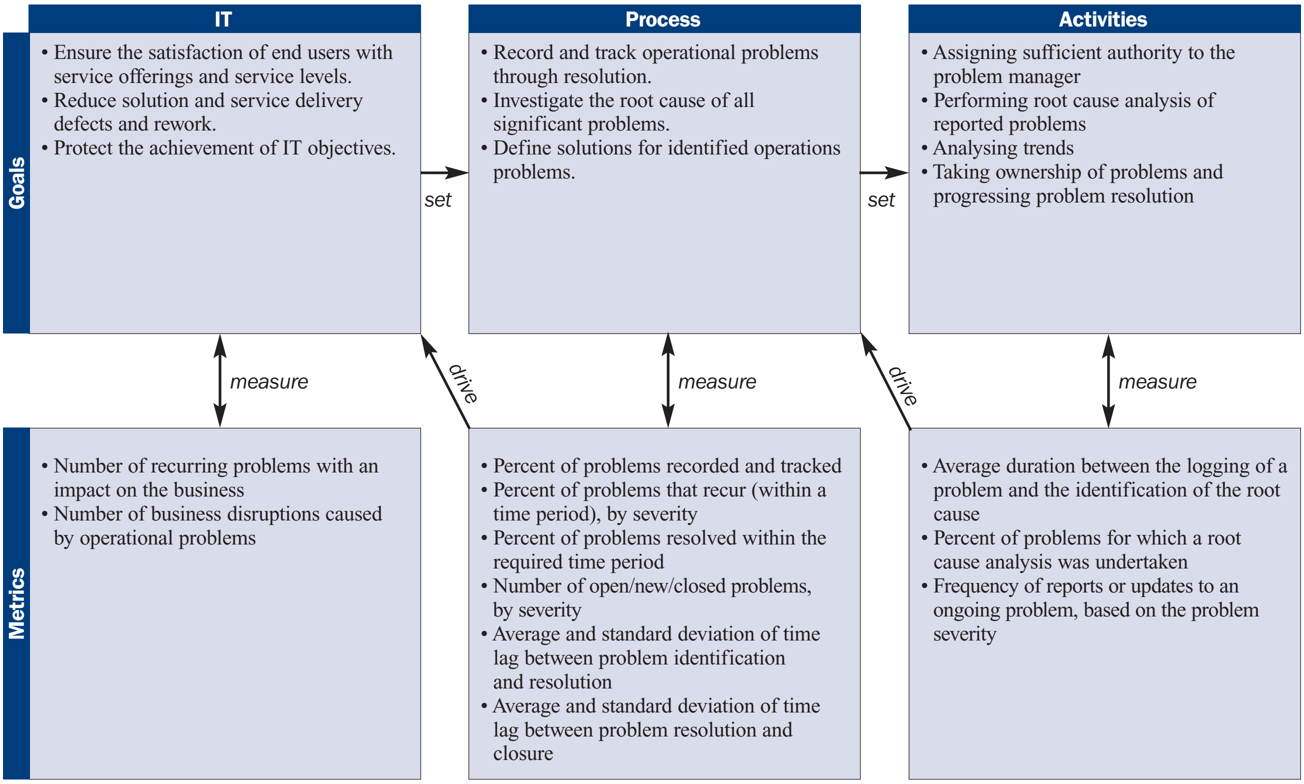
Outputs	To						
Requests for change (where and how to apply the fix)	AI6						
Problem records	AI6						
Process performance reports	ME1						
Known problems, known errors and workarounds	DS8						

RACI Chart

Activities \ Functions	CEO	CFO	Business Executive	CIO	Business Process Owner	Head Operations	Chief Architect	Head Development	Head IT Administration	PMO	Compliance, Audit, Risk and Security	Problem Manager
Identify and classify problems.			I	I	C	A	C	C			I	R
Perform root cause analysis.						C		C				A/R
Resolve problems.					C	A	R	R		R	C	C
Review the status of problems.			I	I	C	A/R	C	C		C	C	R
Issue recommendations for improvement, and create a related RFC.					I	A	I	I		I		R
Maintain problem records.					I	I		I			I	A/R

A **RACI** chart identifies who is **R**esponsible, **A**ccountable, **C**onsulted and/or **I**nformed.

Goals and Metrics



IT – Goals
- Ensure the satisfaction of end users with service offerings and service levels.
- Reduce solution and service delivery defects and rework.
- Protect the achievement of IT objectives.

Process – Goals
- Record and track operational problems through resolution.
- Investigate the root cause of all significant problems.
- Define solutions for identified operations problems.

Activities – Goals
- Assigning sufficient authority to the problem manager
- Performing root cause analysis of reported problems
- Analysing trends
- Taking ownership of problems and progressing problem resolution

IT – Metrics
- Number of recurring problems with an impact on the business
- Number of business disruptions caused by operational problems

Process – Metrics
- Percent of problems recorded and tracked
- Percent of problems that recur (within a time period), by severity
- Percent of problems resolved within the required time period
- Number of open/new/closed problems, by severity
- Average and standard deviation of time lag between problem identification and resolution
- Average and standard deviation of time lag between problem resolution and closure

Activities – Metrics
- Average duration between the logging of a problem and the identification of the root cause
- Percent of problems for which a root cause analysis was undertaken
- Frequency of reports or updates to an ongoing problem, based on the problem severity

Maturity Model

DS10 Manage Problems

Management of the process of *Manage problems* that satisfies the business requirement for IT of *ensuring end users' satisfaction with service offerings and service levels, and reducing solution and service delivery defects and rework* is:

0 Non-existent when
There is no awareness of the need for managing problems, as there is no differentiation of problems and incidents. Therefore, there is no attempt made to identify the root cause of incidents.

1 Initial/*Ad Hoc* when
Personnel recognise the need to manage problems and resolve underlying causes. Key knowledgeable personnel provide some assistance with problems relating to their area of expertise, but the responsibility for problem management is not assigned. Information is not shared, resulting in additional problem creation and loss of productive time while searching for answers.

2 Repeatable but Intuitive when
There is a wide awareness of the need for and benefits of managing IT-related problems within both the business units and information services function. The resolution process is evolved to a point where a few key individuals are responsible for identifying and resolving problems. Information is shared amongst staff in an informal and reactive way. The service level to the user community varies and is hampered by insufficient, structured knowledge available to the problem manager.

3 Defined when
The need for an effective integrated problem management system is accepted and evidenced by management support, and budgets for the staffing and training are available. Problem resolution and escalation processes have been standardised. The recording and tracking of problems and their resolutions are fragmented within the response team, using the available tools without centralisation. Deviations from established norms or standards are likely to be undetected. Information is shared among staff in a proactive and formal manner. Management review of incidents and analysis of problem identification and resolution are limited and informal.

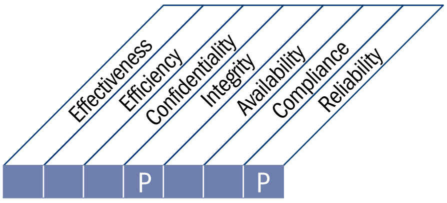
4 Managed and Measurable when
The problem management process is understood at all levels within the organisation. Responsibilities and ownership are clear and established. Methods and procedures are documented, communicated and measured for effectiveness. The majority of problems are identified, recorded and reported, and resolution is initiated. Knowledge and expertise are cultivated, maintained and developed to higher levels, as the function is viewed as an asset and major contributor to the achievement of IT objectives and improvement of IT services. Problem management is well integrated with interrelated processes, such as incident, change, availability and configuration management, and assists customers in managing data, facilities and operations. Goals and metrics have been agreed upon for the problem management process.

5 Optimised when
The problem management process is evolved into a forward-looking and proactive one, contributing to the IT objectives. Problems are anticipated and prevented. Knowledge regarding patterns of past and future problems is maintained through regular contacts with vendors and experts. The recording, reporting and analysis of problems and resolutions are automated and fully integrated with configuration data management. Goals are measured consistently. Most systems have been equipped with automatic detection and warning mechanisms, which are continuously tracked and evaluated. The problem management process is analysed for continuous improvement based on analysis of measures and is reported to stakeholders.

PROCESS DESCRIPTION

DS11 Manage Data

Effective data management requires identifying data requirements. The data management process also includes the establishment of effective procedures to manage the media library, backup and recovery of data, and proper disposal of media. Effective data management helps ensure the quality, timeliness and availability of business data.



Plan and Organise
Acquire and Implement
Deliver and Support
Monitor and Evaluate

Control over the IT process of

Manage data

that satisfies the business requirement for IT of

optimising the use of information and ensuring that information is available as required

by focusing on

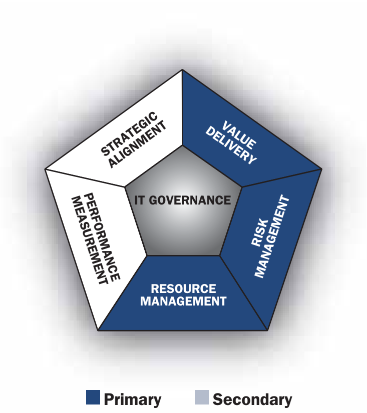
maintaining the completeness, accuracy, availability and protection of data

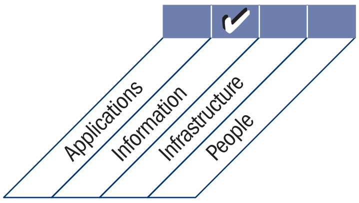
is achieved by

- Backing up data and testing restoration
- Managing onsite and offsite storage of data
- Securely disposing of data and equipment

and is measured by

- Percent of user satisfaction with availability of data
- Percent of successful data restorations
- Number of incidents where sensitive data were retrieved after media were disposed





Control Objectives

DS11 Manage Data

DS11.1 Business Requirements for Data Management
Verify that all data expected for processing are received and processed completely, accurately and in a timely manner, and all output is delivered in accordance with business requirements. Support restart and reprocessing needs.

DS11.2 Storage and Retention Arrangements
Define and implement procedures for effective and efficient data storage, retention and archiving to meet business objectives, the organisation's security policy and regulatory requirements.

DS11.3 Media Library Management System
Define and implement procedures to maintain an inventory of stored and archived media to ensure their usability and integrity.

DS11.4 Disposal
Define and implement procedures to ensure that business requirements for protection of sensitive data and software are met when data and hardware are disposed or transferred.

DS11.5 Backup and Restoration
Define and implement procedures for backup and restoration of systems, applications, data and documentation in line with business requirements and the continuity plan.

DS11.6 Security Requirements for Data Management
Define and implement policies and procedures to identify and apply security requirements applicable to the receipt, processing, storage and output of data to meet business objectives, the organisation's security policy and regulatory requirements.

Management Guidelines

DS11 Manage Data

From	Inputs
PO2	Data dictionary; assigned data classifications
AI4	User, operational, support, technical and administration manuals
DS1	OLAs
DS4	Backup storage and protection plan
DS5	IT security plan and policies

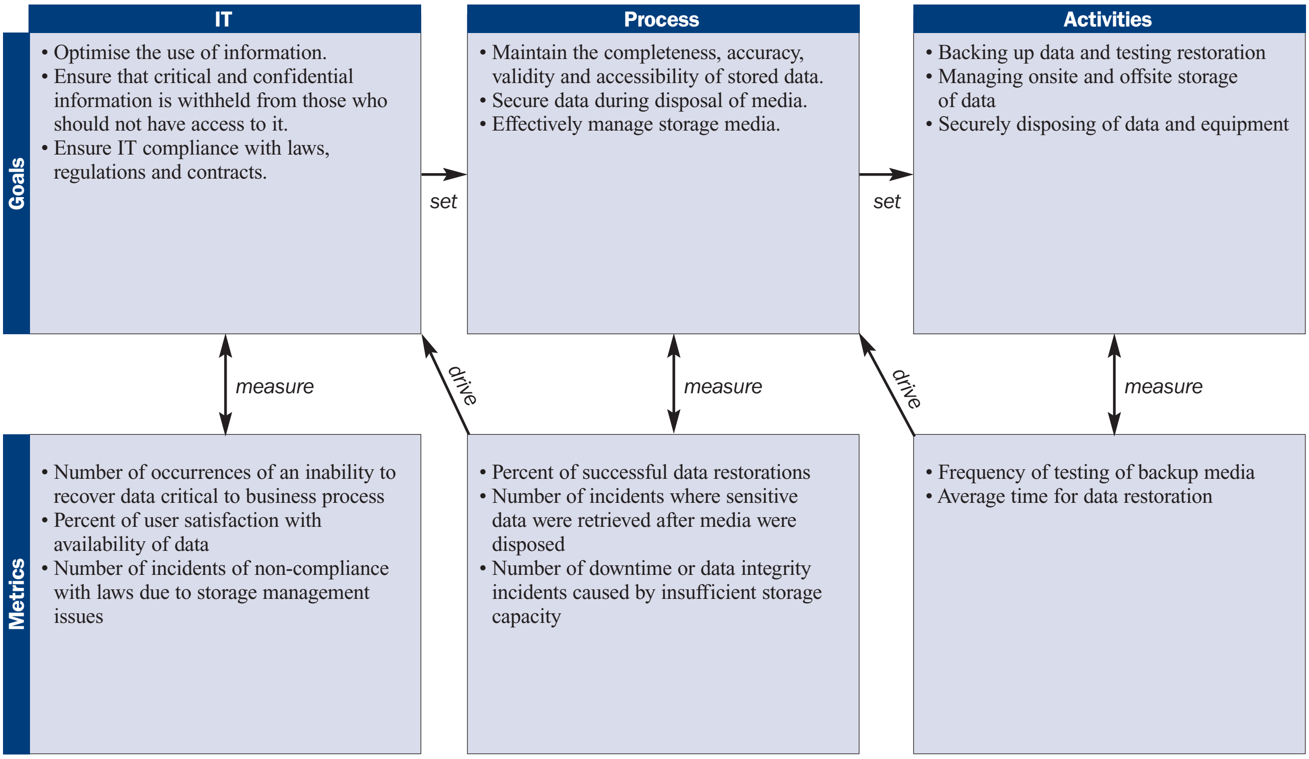
Outputs	To						
Process performance reports	ME1						
Operator instructions for data management	DS13						

RACI Chart

Activities	CEO	CFO	Business Executive	CIO	Business Process Owner	Head Operations	Chief Architect	Head Development	Head IT Administration	PMO	Compliance, Audit, Risk and Security
Translate data storage and retention requirements into procedures.				A	I	C	R				C
Define, maintain and implement procedures to manage the media library.				A		R	C	C	I		C
Define, maintain and implement procedures for secure disposal of media and equipment.				A	C	R			I		C
Back up data according to scheme.				A		R					
Define, maintain and implement procedures for data restoration.				A	C	R	C	C			I

A **RACI** chart identifies who is **R**esponsible, **A**ccountable, **C**onsulted and/or **I**nformed.

Goals and Metrics



IT

Goals

- Optimise the use of information.
- Ensure that critical and confidential information is withheld from those who should not have access to it.
- Ensure IT compliance with laws, regulations and contracts.

Metrics

- Number of occurrences of an inability to recover data critical to business process
- Percent of user satisfaction with availability of data
- Number of incidents of non-compliance with laws due to storage management issues

Process

Goals

- Maintain the completeness, accuracy, validity and accessibility of stored data.
- Secure data during disposal of media.
- Effectively manage storage media.

Metrics

- Percent of successful data restorations
- Number of incidents where sensitive data were retrieved after media were disposed
- Number of downtime or data integrity incidents caused by insufficient storage capacity

Activities

Goals

- Backing up data and testing restoration
- Managing onsite and offsite storage of data
- Securely disposing of data and equipment

Metrics

- Frequency of testing of backup media
- Average time for data restoration

Maturity Model

DS11 Manage Data

Management of the process of *Manage data* that satisfies the business requirement for IT of *optimising the use of information and ensuring that information is available as required* is:

0 Non-existent when
Data are not recognised as corporate resources and assets. There is no assigned data ownership or individual accountability for data management. Data quality and security are poor or non-existent.

1 Initial/*Ad Hoc* when
The organisation recognises a need for effective data management. There is an *ad hoc* approach for specifying security requirements for data management, but no formal communications procedures are in place. No specific training on data management takes place. Responsibility for data management is not clear. Backup/restoration procedures and disposal arrangements are in place.

2 Repeatable but Intuitive when
The awareness of the need for effective data management exists throughout the organisation. Data ownership at a high level begins to occur. Security requirements for data management are documented by key individuals. Some monitoring within IT is performed on data management key activities (e.g., backup, restoration, disposal). Responsibilities for data management are informally assigned for key IT staff members.

3 Defined when
The need for data management within IT and across the organisation is understood and accepted. Responsibility for data management is established. Data ownership is assigned to the responsible party who controls integrity and security. Data management procedures are formalised within IT, and some tools for backup/restoration and disposal of equipment are used. Some monitoring over data management is in place. Basic performance metrics are defined. Training for data management staff members is emerging.

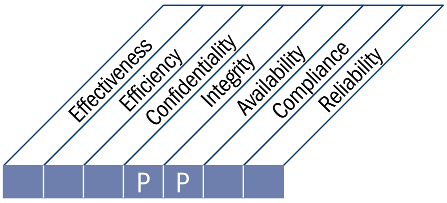
4 Managed and Measurable when
The need for data management is understood, and required actions are accepted within the organisation. Responsibility for data ownership and management are clearly defined, assigned and communicated within the organisation. Procedures are formalised and widely known, and knowledge is shared. Usage of current tools is emerging. Goal and performance indicators are agreed to with customers and monitored through a well-defined process. Formal training for data management staff members is in place.

5 Optimised when
The need for data management and the understanding of all required actions is understood and accepted within the organisation. Future needs and requirements are explored in a proactive manner. The responsibilities for data ownership and data management are clearly established, widely known across the organisation and updated on a timely basis. Procedures are formalised and widely known, and knowledge sharing is standard practice. Sophisticated tools are used with maximum automation of data management. Goal and performance indicators are agreed to with customers, linked to business objectives and consistently monitored using a well-defined process. Opportunities for improvement are constantly explored. Training for data management staff members is instituted.

Process Description

DS12 Manage the Physical Environment

Protection for computer equipment and personnel requires well-designed and well-managed physical facilities. The process of managing the physical environment includes defining the physical site requirements, selecting appropriate facilities, and designing effective processes for monitoring environmental factors and managing physical access. Effective management of the physical environment reduces business interruptions from damage to computer equipment and personnel.



Plan and Organise
Acquire and Implement
Deliver and Support
Monitor and Evaluate

Control over the IT process of

Manage the physical environment

that satisfies the business requirement for IT of

protecting computer assets and business data and minimising the risk of business disruption

by focusing on

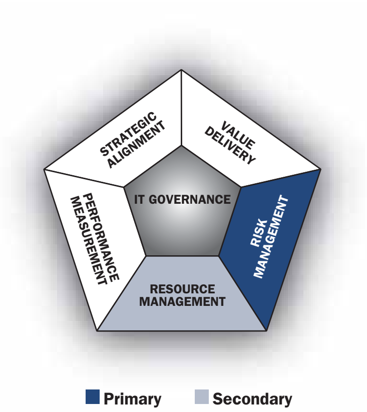
providing and maintaining a suitable physical environment to protect IT assets from access, damage or theft

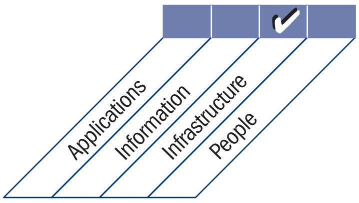
is achieved by

- Implementing physical security measures
- Selecting and managing facilities

and is measured by

- Amount of downtime arising from physical environment incidents
- Number of incidents due to physical security breaches or failures
- Frequency of physical risk assessment and reviews





Control Objectives

DS12 Manage the Physical Environment

DS12.1 Site Selection and Layout
Define and select the physical sites for IT equipment to support the technology strategy linked to the business strategy. The selection and design of the layout of a site should take into account the risk associated with natural and man-made disasters, whilst considering relevant laws and regulations, such as occupational health and safety regulations.

DS12.2 Physical Security Measures
Define and implement physical security measures in line with business requirements to secure the location and the physical assets. Physical security measures must be capable of effectively preventing, detecting and mitigating risks relating to theft, temperature, fire, smoke, water, vibration, terror, vandalism, power outages, chemicals or explosives.

DS12.3 Physical Access
Define and implement procedures to grant, limit and revoke access to premises, buildings and areas according to business needs, including emergencies. Access to premises, buildings and areas should be justified, authorised, logged and monitored. This should apply to all persons entering the premises, including staff, temporary staff, clients, vendors, visitors or any other third party.

DS12.4 Protection Against Environmental Factors
Design and implement measures for protection against environmental factors. Install specialised equipment and devices to monitor and control the environment.

DS12.5 Physical Facilities Management
Manage facilities, including power and communications equipment, in line with laws and regulations, technical and business requirements, vendor specifications, and health and safety guidelines.

Management Guidelines

DS12 Manage the Physical Environment

From	Inputs
PO2	Assigned data classifications
PO9	Risk assessment
AI3	Physical environment requirements

Outputs	To						
Process performance reports	ME1						

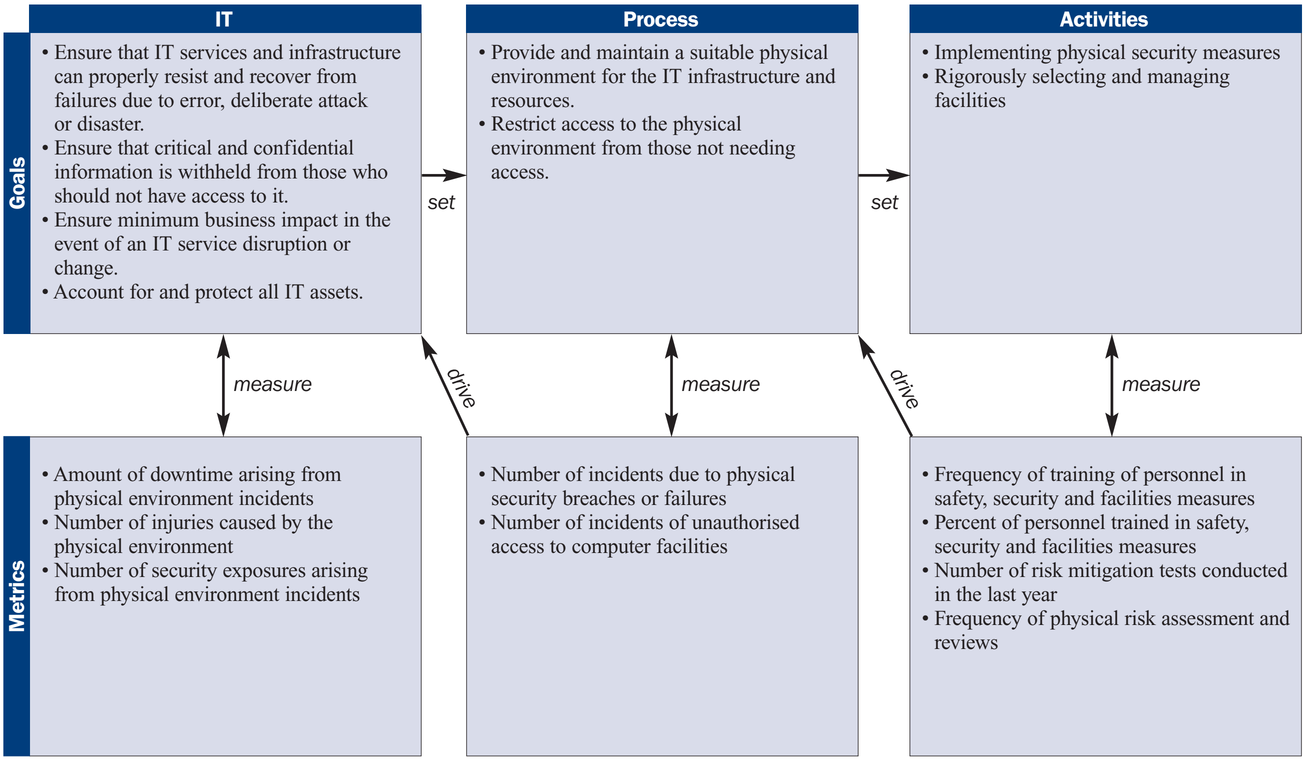
RACI Chart

Functions

Activities	CEO	CFO	Business Executive	CIO	Business Process Owner	Head Operations	Chief Architect	Head Development	Head IT Administration	PMO	Compliance, Audit, Risk and Security
Define the required level of physical protection.					C	A/R	C				C
Select and commission the site (data center, office, etc.).	I	C	C	C	C	A/R	C		C	C	C
Implement physical environment measures.					I	A/R	I	I			C
Manage the physical environment (maintaining, monitoring and reporting included).						A/R	C				
Define and implement procedures for physical access authorisation and maintenance.				C	I	A/R	I	I	I		C

A **RACI** chart identifies who is **R**esponsible, **A**ccountable, **C**onsulted and/or **I**nformed.

Goals and Metrics



IT (Goals)

- Ensure that IT services and infrastructure can properly resist and recover from failures due to error, deliberate attack or disaster.
- Ensure that critical and confidential information is withheld from those who should not have access to it.
- Ensure minimum business impact in the event of an IT service disruption or change.
- Account for and protect all IT assets.

Process (Goals)

- Provide and maintain a suitable physical environment for the IT infrastructure and resources.
- Restrict access to the physical environment from those not needing access.

Activities (Goals)

- Implementing physical security measures
- Rigorously selecting and managing facilities

IT (Metrics)

- Amount of downtime arising from physical environment incidents
- Number of injuries caused by the physical environment
- Number of security exposures arising from physical environment incidents

Process (Metrics)

- Number of incidents due to physical security breaches or failures
- Number of incidents of unauthorised access to computer facilities

Activities (Metrics)

- Frequency of training of personnel in safety, security and facilities measures
- Percent of personnel trained in safety, security and facilities measures
- Number of risk mitigation tests conducted in the last year
- Frequency of physical risk assessment and reviews

Maturity Model

DS12 Manage the Physical Environment

Management of the process of *Manage the physical environment* that satisfies the business requirement for IT of *protecting computer assets and business data and minimising the risk of business disruption* is:

0 Non-existent when
There is no awareness of the need to protect the facilities or the investment in computing resources. Environmental factors, including fire protection, dust, power, and excessive heat and humidity, are neither monitored nor controlled.

1 Initial/*Ad Hoc* when
The organisation recognises a business requirement to provide a suitable physical environment that protects the resources and personnel against man-made and natural hazards. The management of facilities and equipment is dependent upon the skills and abilities of key individuals. Personnel can move within the facilities without restriction. Management does not monitor the facility environmental controls or the movement of personnel.

2 Repeatable but Intuitive when
Environmental controls are implemented and monitored by the operations personnel. Physical security is an informal process, driven by a small group of employees possessing a high level of concern about securing the physical facilities. The facilities maintenance procedures are not well documented and rely upon good practices of a few individuals. The physical security goals are not based on any formal standards, and management does not ensure that security objectives are achieved.

3 Defined when
The need to maintain a controlled computing environment is understood and accepted within the organisation. Environmental controls, preventive maintenance and physical security are budget items approved and tracked by management. Access restrictions are applied, with only approved personnel allowed access to the computing facilities. Visitors are logged and escorted, depending on the individual. The physical facilities are low-profile and not readily identifiable. Civil authorities monitor compliance with health and safety regulations. The risks are insured with minimal effort to optimise the insurance costs.

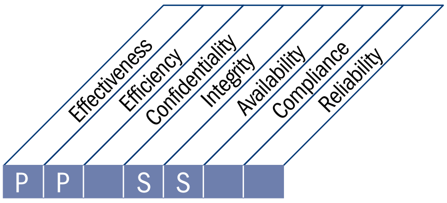
4 Managed and Measurable when
The need to maintain a controlled computing environment is fully understood, as evident in the organisational structure and budget allocations. Environmental and physical security requirements are documented, and access is strictly controlled and monitored. Responsibility and ownership are established and communicated. The facilities staff members are fully trained in emergency situations, as well as in health and safety practices. Standardised control mechanisms are in place for restricting access to facilities and addressing environmental and safety factors. Management monitors the effectiveness of controls and compliance with established standards. Management has established goals and metrics for measuring management of the computing environment. The recoverability of computing resources is incorporated into an organisational risk management process. The integrated information is used to optimise insurance coverage and related costs.

5 Optimised when
There is an agreed-upon, long-term plan for the facilities required to support the organisation's computing environment. Standards are defined for all facilities, covering site selection, construction, guarding, personnel safety, mechanical and electrical systems, and protection against environmental factors (e.g., fire, lighting, flooding). All facilities are inventoried and classified according to the organisation's ongoing risk management process. Access is strictly controlled on a job-need basis and monitored continuously, and all visitors are escorted at all times. The environment is monitored and controlled through specialised equipment, and equipment rooms have become 'unmanned'. Goals are consistently measured and evaluated. Preventive maintenance programmes enforce a strict adherence to schedules, and regular tests are applied to sensitive equipment. The facilities strategy and standards are aligned with IT services availability targets and integrated with business continuity planning and crisis management. Management reviews and optimises the facilities using goals and metrics on a continual basis, capitalising on opportunities to improve the business contribution.

Process Description

DS13 Manage Operations

Complete and accurate processing of data requires effective management of data processing procedures and diligent maintenance of hardware. This process includes defining operating policies and procedures for effective management of scheduled processing, protecting sensitive output, monitoring infrastructure performance and ensuring preventive maintenance of hardware. Effective operations management helps maintain data integrity and reduces business delays and IT operating costs.



Plan and Organise
Acquire and Implement
Deliver and Support
Monitor and Evaluate

Control over the IT process of

Manage operations

that satisfies the business requirement for IT of

maintaining data integrity and ensuring that IT infrastructure can resist and recover from errors and failures

by focusing on

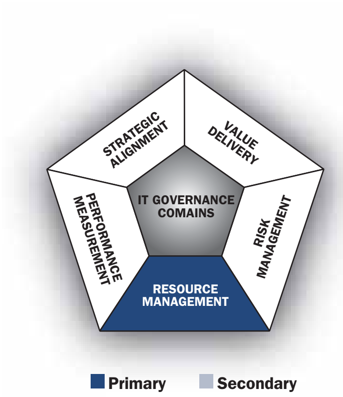
meeting operational service levels for scheduled data processing, protecting sensitive output, and monitoring and maintaining infrastructure

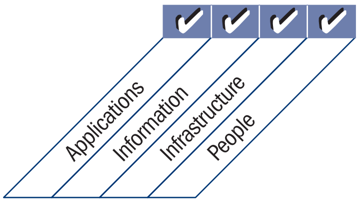
is achieved by

- Operating the IT environment in line with agreed-upon service levels and defined instructions
- Maintaining the IT infrastructure

and is measured by

- Number of service levels impacted by operational incidents
- Hours of unplanned downtime caused by operational incidents
- Percent of hardware assets included in preventive maintenance schedules





Control Objectives

DS13 Manage Operations

DS13.1 Operations Procedures and Instructions

Define, implement and maintain procedures for IT operations, ensuring that the operations staff members are familiar with all operations tasks relevant to them. Operational procedures should cover shift handover (formal handover of activity, status updates, operational problems, escalation procedures and reports on current responsibilities) to support agreed-upon service levels and ensure continuous operations.

DS13.2 Job Scheduling

Organise the scheduling of jobs, processes and tasks into the most efficient sequence, maximising throughput and utilisation to meet business requirements.

DS13.3 IT Infrastructure Monitoring

Define and implement procedures to monitor the IT infrastructure and related events. Ensure that sufficient chronological information is being stored in operations logs to enable the reconstruction, review and examination of the time sequences of operations and the other activities surrounding or supporting operations.

DS13.4 Sensitive Documents and Output Devices

Establish appropriate physical safeguards, accounting practices and inventory management over sensitive IT assets, such as special forms, negotiable instruments, special purpose printers or security tokens.

DS13.5 Preventive Maintenance for Hardware

Define and implement procedures to ensure timely maintenance of infrastructure to reduce the frequency and impact of failures or performance degradation.

Management Guidelines

DS13 Manage Operations

From	Inputs
AI4	User, operational, support, technical and administration manuals
AI7	Promotion to production and software release and distribution plans
DS1	SLAs and OLAs
DS4	Backup storage and protection plan
DS9	IT configuration/assets details
DS11	Operator instructions for data management

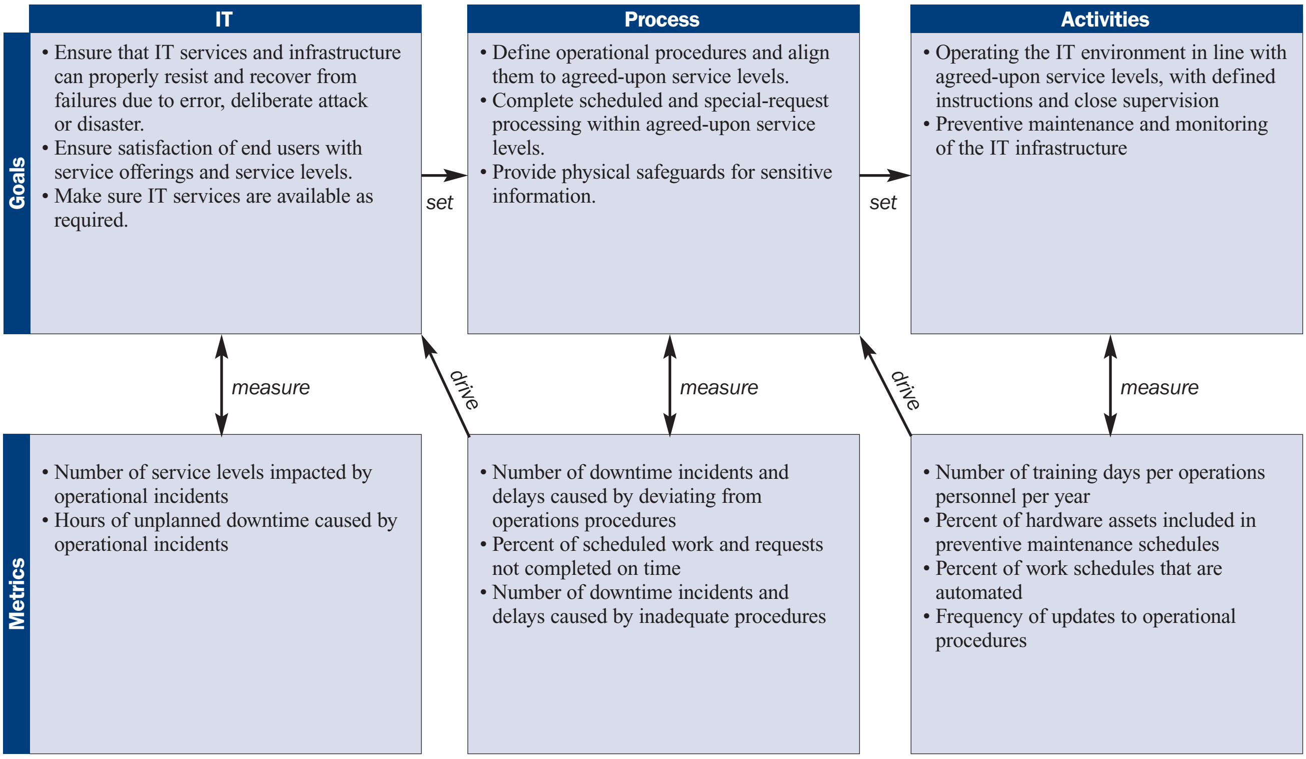
Outputs	To					
Incident tickets	DS8					
Error logs	DS10					
Process performance reports	ME1					

RACI Chart

Activities / Functions	CEO	CFO	Business Executive	CIO	Business Process Owner	Head Operations	Chief Architect	Head Development	Head IT Administration	PMO	Compliance, Audit, Risk and Security
Create/modify operations procedures (including manuals, checklists, shift planning, handover documentation, escalation procedures, etc.).						A/R					I
Schedule workload and batch jobs.					C	A/R	C	C			
Monitor infrastructure and processing, and resolve problems.						A/R					I
Manage and secure physical output (e.g., paper, media).						A/R					C
Apply fixes or changes to the schedule and infrastructure.					C	A/R	C	C			C
Implement/establish a process for safeguarding authentication devices against interference, loss and theft.				A		R			I		C
Schedule and perform preventive maintenance.						A/R					

A **RACI** chart identifies who is **R**esponsible, **A**ccountable, **C**onsulted and/or **I**nformed.

Goals and Metrics



IT

Goals:
- Ensure that IT services and infrastructure can properly resist and recover from failures due to error, deliberate attack or disaster.
- Ensure satisfaction of end users with service offerings and service levels.
- Make sure IT services are available as required.

Metrics:
- Number of service levels impacted by operational incidents
- Hours of unplanned downtime caused by operational incidents

Process

Goals:
- Define operational procedures and align them to agreed-upon service levels.
- Complete scheduled and special-request processing within agreed-upon service levels.
- Provide physical safeguards for sensitive information.

Metrics:
- Number of downtime incidents and delays caused by deviating from operations procedures
- Percent of scheduled work and requests not completed on time
- Number of downtime incidents and delays caused by inadequate procedures

Activities

Goals:
- Operating the IT environment in line with agreed-upon service levels, with defined instructions and close supervision
- Preventive maintenance and monitoring of the IT infrastructure

Metrics:
- Number of training days per operations personnel per year
- Percent of hardware assets included in preventive maintenance schedules
- Percent of work schedules that are automated
- Frequency of updates to operational procedures

Maturity Model

DS13 Manage Operations

Management of the process of *Manage operations* that satisfies the business requirement for IT of *maintaining data integrity and ensuring that IT infrastructure can resist and recover from errors and failures* is:

0 Non-existent when
The organisation does not devote time and resources to the establishment of basic IT support and operations activities.

1 Initial/*Ad Hoc* when
The organisation recognises the need for structuring the IT support functions. Few standard procedures are established, and the operations activities are reactive in nature. The majority of operational processes are informally scheduled, and processing requests are accepted without prior validation. Computers, systems and applications supporting the business processes are frequently interrupted, delayed and unavailable. Time is lost while employees wait for resources. Output media sometimes show up in unexpected places or not at all.

2 Repeatable but Intuitive when
The organisation is aware of the key role that IT operations activities play in providing IT support functions. Budgets for tools are being allocated on a case-by-case basis. IT support operations are informal and intuitive. There is a high dependence on the skills and abilities of individuals. The instructions covering what to do, when and in what order are not documented. Some operator training exists, and there are some formal operating standards.

3 Defined when
The need for computer operations management is understood and accepted within the organisation. Resources are allocated and some on-the-job training occurs. Repeatable functions are formally defined, standardised, documented and communicated. The events and completed task results are recorded, with limited reporting to management. The use of automated scheduling and other tools is introduced to limit operator intervention. Controls are introduced for the placement of new jobs in operations. A formal policy is developed to reduce the number of unscheduled events. Maintenance and service agreements with vendors are still informal in nature.

4 Managed and Measurable when
The computer operations and support responsibilities are clearly defined and ownership is assigned. Operations are supported through resource budgets for capital expenditures and human resources. Training is formalised and ongoing. Schedules and tasks are documented and communicated, both internally to the IT function and to the business customers. It is possible to measure and monitor the daily activities with standardised performance agreements and established service levels. Any deviations from established norms are quickly addressed and corrected. Management monitors the use of computing resources and completion of work or assigned tasks. An ongoing effort exists to increase the level of process automation as a means of continuous improvement. Formal maintenance and service agreements are established with vendors. There is full alignment with problem, capacity and availability management processes, supported by an analysis of the causes of errors and failures.

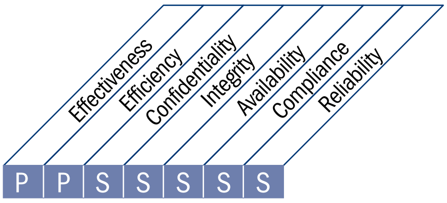
5 Optimised when
IT support operations are effective, efficient and sufficiently flexible to meet service level needs with minimal lost productivity. Operational IT management processes are standardised and documented in a knowledge base and are subject to continuous improvement. Automated processes that support systems operate seamlessly and contribute to a stable environment. All problems and failures are analysed to identify the root cause. Regular meetings with change management ensure timely inclusion of changes in production schedules. In co-operation with vendors, equipment is analysed for age and malfunction symptoms, and maintenance is mainly preventive in nature.

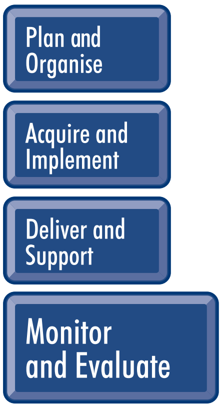
Monitor and Evaluate

Process Description

ME1 Monitor and Evaluate IT Performance

Effective IT performance management requires a monitoring process. This process includes defining relevant performance indicators, systematic and timely reporting of performance, and prompt acting upon deviations. Monitoring is needed to make sure that the right things are done and are in line with the set directions and policies.





Control over the IT process of

Monitor and evaluate IT performance

that satisfies the business requirement for IT of

transparency and understanding of IT cost, benefits, strategy, policies and service levels in accordance with governance requirements

by focusing on

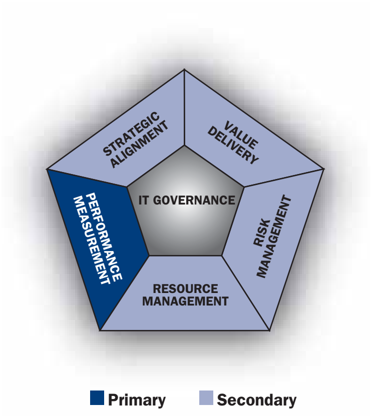
monitoring and reporting process metrics and identifying and implementing performance improvement actions

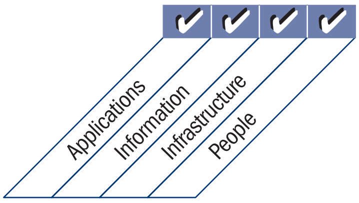
is achieved by

- Collating and translating process performance reports into management reports
- Reviewing performance against agreed-upon targets and initiating necessary remedial action

and is measured by

- Satisfaction of management and the governance entity with the performance reporting
- Number of improvement actions driven by monitoring activities
- Percent of critical processes monitored





Control Objectives

ME1 Monitor and Evaluate IT Performance

ME1.1 Monitoring Approach

Establish a general monitoring framework and approach to define the scope, methodology and process to be followed for measuring IT's solution and service delivery, and monitor IT's contribution to the business. Integrate the framework with the corporate performance management system.

ME1.2 Definition and Collection of Monitoring Data

Work with the business to define a balanced set of performance targets and have them approved by the business and other relevant stakeholders. Define benchmarks with which to compare the targets, and identify available data to be collected to measure the targets. Establish processes to collect timely and accurate data to report on progress against targets.

ME1.3 Monitoring Method

Deploy a performance monitoring method (e.g., balanced scorecard) that records targets; captures measurements; provides a succinct, all-around view of IT performance; and fits within the enterprise monitoring system.

ME1.4 Performance Assessment

Periodically review performance against targets, analyse the cause of any deviations, and initiate remedial action to address the underlying causes. At appropriate times, perform root cause analysis across deviations.

ME1.5 Board and Executive Reporting

Develop senior management reports on IT's contribution to the business, specifically in terms of the performance of the enterprise's portfolio, IT-enabled investment programmes, and the solution and service deliverable performance of individual programmes. Include in status reports the extent to which planned objectives have been achieved, budgeted resources used, set performance targets met and identified risks mitigated. Anticipate senior management's review by suggesting remedial actions for major deviations. Provide the report to senior management, and solicit feedback from management's review.

ME1.6 Remedial Actions

Identify and initiate remedial actions based on performance monitoring, assessment and reporting. This includes follow-up of all monitoring, reporting and assessments through:

- Review, negotiation and establishment of management responses
- Assignment of responsibility for remediation
- Tracking of the results of actions committed

Management Guidelines

ME1 Monitor and Evaluate IT Performance

From	Inputs
PO5	Cost-benefit reports
PO10	Project performance reports
AI6	Change status reports
DS1-13	Process performance reports
DS3	Peformance and capacity plan (requirements)
DS8	User satisfaction reports
ME2	Report on effectiveness of IT controls
ME3	Report on compliance of IT activities with external legal and regulatory requirements
ME4	Report on IT governance status

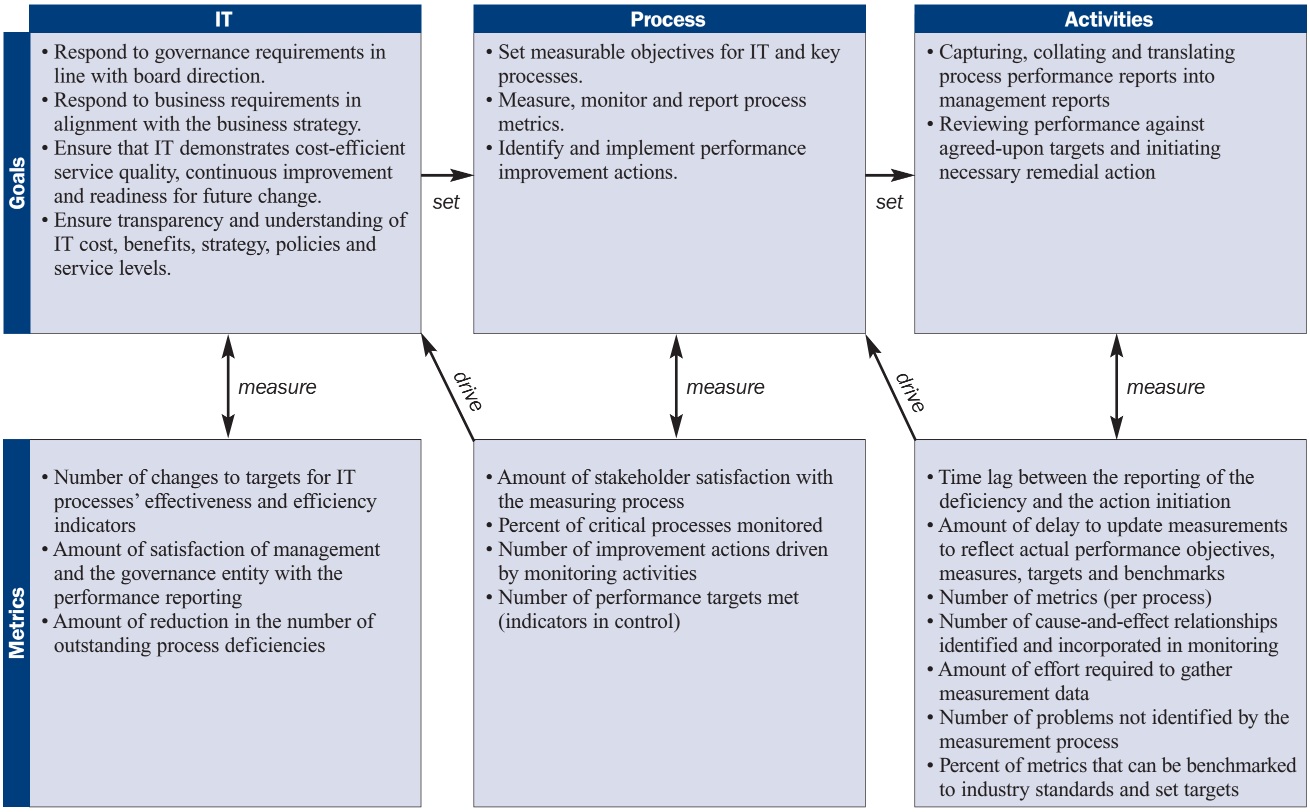
Outputs	To						
Performance input to IT planning	PO1	PO2	DS1				
Remedial action plans	PO4	PO8					
Historical risk trends and events	PO9						
Process performance report	ME2						

RACI Chart

Activities	Board	CEO	CFO	Business Executive	CIO	Business Process Owner	Head Operations	Chief Architect	Head Development	Head IT Administration	PMO	Compliance, Audit, Risk and Security
Establish the monitoring approach.		A	R	C	R	I	C	I	C	I		C
Identify and collect measureable objectives that support the business objectives.		C	C	C	A	R	R		R			
Create scorecards.					A		R	C	R	C		
Assess performance.			I	I	A	R	R	C	R	C		
Report performance.	I	I	I	R	A	R	R	C	R	C		I
Identify and monitor performance improvement actions.					A	R	R	C	R	C		C

A **RACI** chart identifies who is **R**esponsible, **A**ccountable, **C**onsulted and/or **I**nformed.

Goals and Metrics



IT

Goals
- Respond to governance requirements in line with board direction.
- Respond to business requirements in alignment with the business strategy.
- Ensure that IT demonstrates cost-efficient service quality, continuous improvement and readiness for future change.
- Ensure transparency and understanding of IT cost, benefits, strategy, policies and service levels.

Metrics
- Number of changes to targets for IT processes' effectiveness and efficiency indicators
- Amount of satisfaction of management and the governance entity with the performance reporting
- Amount of reduction in the number of outstanding process deficiencies

Process

Goals
- Set measurable objectives for IT and key processes.
- Measure, monitor and report process metrics.
- Identify and implement performance improvement actions.

Metrics
- Amount of stakeholder satisfaction with the measuring process
- Percent of critical processes monitored
- Number of improvement actions driven by monitoring activities
- Number of performance targets met (indicators in control)

Activities

Goals
- Capturing, collating and translating process performance reports into management reports
- Reviewing performance against agreed-upon targets and initiating necessary remedial action

Metrics
- Time lag between the reporting of the deficiency and the action initiation
- Amount of delay to update measurements to reflect actual performance objectives, measures, targets and benchmarks
- Number of metrics (per process)
- Number of cause-and-effect relationships identified and incorporated in monitoring
- Amount of effort required to gather measurement data
- Number of problems not identified by the measurement process
- Percent of metrics that can be benchmarked to industry standards and set targets

Maturity Model

ME1 Monitor and Evaluate IT Performance

Management of the process of *Monitor and evaluate IT performance* that satisfies the business requirement for IT of *transparency and understanding of IT cost, benefits, strategy, policies and service levels in accordance with governance requirements* is:

0 Non-existent when
The organisation has no monitoring process implemented. IT does not independently perform monitoring of projects or processes. Useful, timely and accurate reports are not available. The need for clearly understood process objectives is not recognised.

1 Initial/*Ad Hoc* when
Management recognises a need to collect and assess information about monitoring processes. Standard collection and assessment processes have not been identified. Monitoring is implemented and metrics are chosen on a case-by-case basis, according to the needs of specific IT projects and processes. Monitoring is generally implemented reactively to an incident that has caused some loss or embarrassment to the organisation. The accounting function monitors basic financial measures for IT.

2 Repeatable but Intuitive when
Basic measurements to be monitored are identified. Collection and assessment methods and techniques exist, but the processes are not adopted across the entire organisation. Interpretation of monitoring results is based on the expertise of key individuals. Limited tools are chosen and implemented for gathering information, but the gathering is not based on a planned approach.

3 Defined when
Management communicates and institutes standard monitoring processes. Educational and training programmes for monitoring are implemented. A formalised knowledge base of historical performance information is developed. Assessment is still performed at the individual IT process and project level and is not integrated amongst all processes. Tools for monitoring IT processes and service levels are defined. Measurements of the contribution of the information services function to the performance of the organisation are defined, using traditional financial and operational criteria. IT-specific performance measurements, non-financial measurements, strategic measurements, customer satisfaction measurements and service levels are defined. A framework is defined for measuring performance.

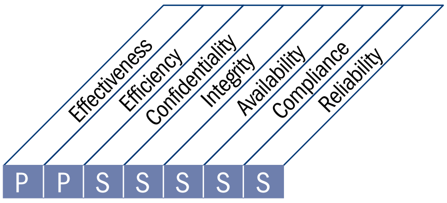
4 Managed and Measurable when
Management defines the tolerances under which processes must operate. Reporting of monitoring results is being standardised and normalised. There is integration of metrics across all IT projects and processes. The IT organisation's management reporting systems are formalised. Automated tools are integrated and leveraged organisationwide to collect and monitor operational information on applications, systems and processes. Management is able to evaluate performance based on agreed-upon criteria approved by stakeholders. Measurements of the IT function align with organisationwide goals.

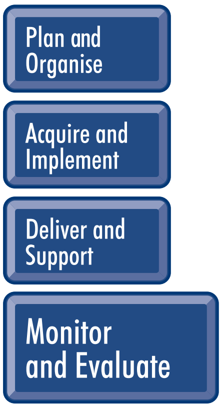
5 Optimised when
A continuous quality improvement process is developed for updating organisationwide monitoring standards and policies and incorporating industry good practices. All monitoring processes are optimised and support organisationwide objectives. Business-driven metrics are routinely used to measure performance and are integrated into strategic assessment frameworks, such as the IT balanced scorecard. Process monitoring and ongoing redesign are consistent with organisationwide business process improvement plans. Benchmarking against industry and key competitors becomes formalised, with well-understood comparison criteria.

Process Description

ME2 Monitor and Evaluate Internal Control

Establishing an effective internal control programme for IT requires a well-defined monitoring process. This process includes the monitoring and reporting of control exceptions, results of self-assessments and third-party reviews. A key benefit of internal control monitoring is to provide assurance regarding effective and efficient operations and compliance with applicable laws and regulations.





Control over the IT process of

Monitor and evaluate internal control

that satisfies the business requirement for IT of

protecting the achievement of IT objectives and complying with IT-related laws, regulations and contracts

by focusing on

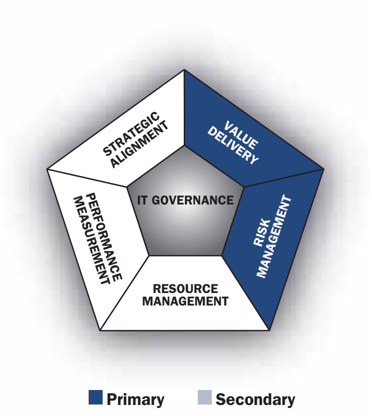
monitoring the internal control processes for IT-related activities and identifying improvement actions

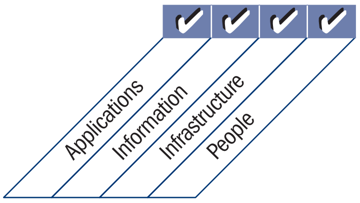
is achieved by

- Defining a system of internal controls embedded in the IT process framework
- Monitoring and reporting on the effectiveness of the internal controls over IT
- Reporting control exceptions to management for action

and is measured by

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





Control Objectives

ME2 Monitor and Evaluate Internal Control

ME2.1 Monitoring of Internal Control Framework
Continuously monitor, benchmark and improve the IT control environment and control framework to meet organisational objectives.

ME2.2 Supervisory Review
Monitor and evaluate the efficiency and effectiveness of internal IT managerial review controls.

ME2.3 Control Exceptions
Identify control exceptions, and analyse and identify their underlying root causes. Escalate control exceptions and report to stakeholders appropriately. Institute necessary corrective action.

ME2.4 Control Self-assessment
Evaluate the completeness and effectiveness of management's control over IT processes, policies and contracts through a continuing programme of self-assessment.

ME2.5 Assurance of Internal Control
Obtain, as needed, further assurance of the completeness and effectiveness of internal controls through third-party reviews.

ME2.6 Internal Control at Third Parties
Assess the status of external service providers' internal controls. Confirm that external service providers comply with legal and regulatory requirements and contractual obligations.

ME2.7 Remedial Actions
Identify, initiate, track and implement remedial actions arising from control assessments and reporting.

Management Guidelines

ME2 Monitor and Evaluate Internal Control

From	Inputs
AI7	Internal control monitoring
ME1	Process performance report

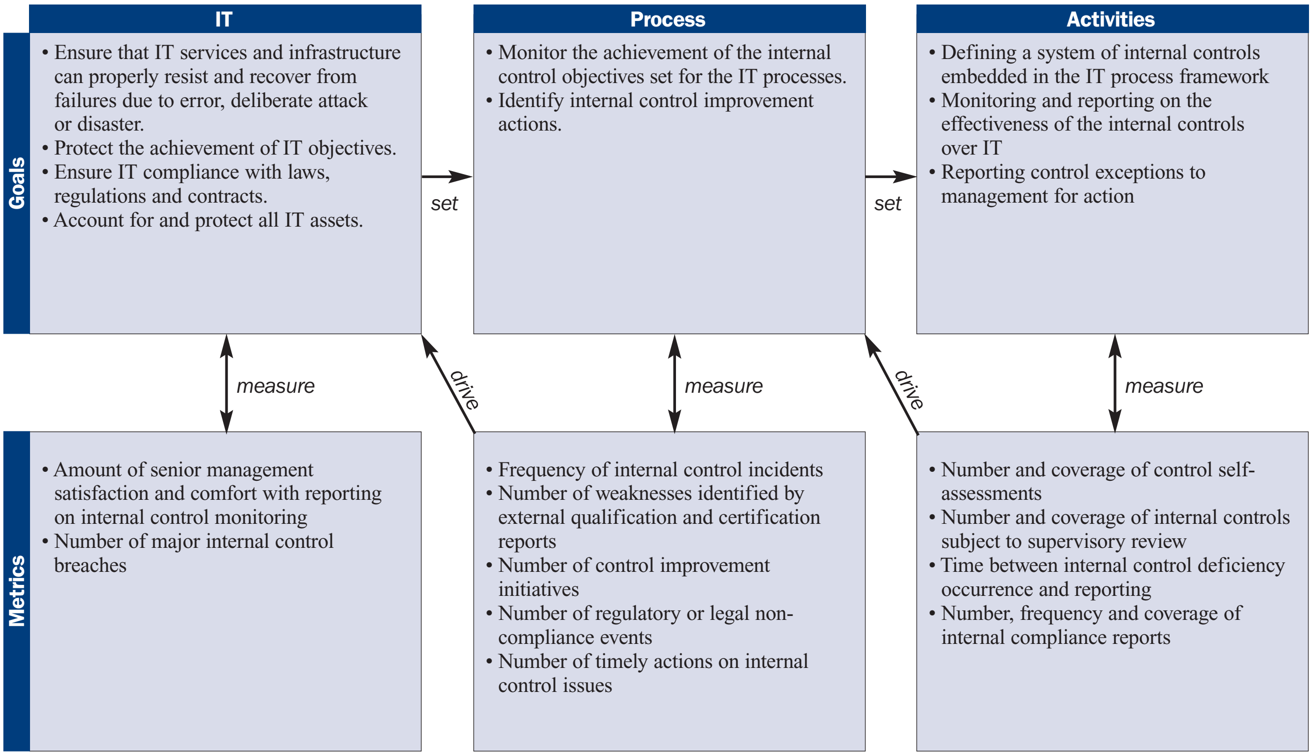
Outputs	To						
Report on effectiveness of IT controls	PO4	PO6	ME1	ME4			

RACI Chart

Activities	Board	CEO	CFO	Business Executive	CIO	Business Process Owner	Head Operations	Chief Architect	Head Development	Head IT Administration	PMO	Compliance, Audit, Risk and Security
Monitor and control IT internal control activities.					A		R		R	R		R
Monitor the self-assessment process.				I	A		R		R	R		C
Monitor the performance of independent reviews, audits and examinations.				I	A		R		R	R		C
Monitor the process to obtain assurance over controls operated by third parties.		I	I	I	A		R		R	R		C
Monitor the process to identify and assess control exceptions.		I	I	I	A	I	R		R	R		C
Monitor the process to identify and remediate control exceptions.		I	I	I	A	I	R		R	R		C
Report to key stakeholders.	I	I	I		A/R							I

A **RACI** chart identifies who is **R**esponsible, **A**ccountable, **C**onsulted and/or **I**nformed.

Goals and Metrics



IT

- Ensure that IT services and infrastructure can properly resist and recover from failures due to error, deliberate attack or disaster.
- Protect the achievement of IT objectives.
- Ensure IT compliance with laws, regulations and contracts.
- Account for and protect all IT assets.

Process

- Monitor the achievement of the internal control objectives set for the IT processes.
- Identify internal control improvement actions.

Activities

- Defining a system of internal controls embedded in the IT process framework
- Monitoring and reporting on the effectiveness of the internal controls over IT
- Reporting control exceptions to management for action

- Amount of senior management satisfaction and comfort with reporting on internal control monitoring
- Number of major internal control breaches

- Frequency of internal control incidents
- Number of weaknesses identified by external qualification and certification reports
- Number of control improvement initiatives
- Number of regulatory or legal non-compliance events
- Number of timely actions on internal control issues

- Number and coverage of control self-assessments
- Number and coverage of internal controls subject to supervisory review
- Time between internal control deficiency occurrence and reporting
- Number, frequency and coverage of internal compliance reports

Maturity Model

ME2 Monitor and Evaluate Internal Control

Management of the process of *Monitor and evaluate internal control* that satisfies the business requirement for IT of *protecting the achievement of IT objectives and complying with IT-related laws and regulations* is:

0 Non-existent when
The organisation lacks procedures to monitor the effectiveness of internal controls. Management internal control reporting methods are absent. There is a general unawareness of IT operational security and internal control assurance. Management and employees have an overall lack of awareness of internal controls.

1 Initial/*Ad Hoc* when
Management recognises the need for regular IT management and control assurance. Individual expertise in assessing internal control adequacy is applied on an *ad hoc* basis. IT management has not formally assigned responsibility for monitoring the effectiveness of internal controls. IT internal control assessments are conducted as part of traditional financial audits, with methodologies and skill sets that do not reflect the needs of the information services function.

2 Repeatable but Intuitive when
The organisation uses informal control reports to initiate corrective action initiatives. Internal control assessment is dependent on the skill sets of key individuals. The organisation has an increased awareness of internal control monitoring. Information service management performs monitoring over the effectiveness of what it believes are critical internal controls on a regular basis. Methodologies and tools for monitoring internal controls are starting to be used, but not based on a plan. Risk factors specific to the IT environment are identified based on the skills of individuals.

3 Defined when
Management supports and institutes internal control monitoring. Policies and procedures are developed for assessing and reporting on internal control monitoring activities. An education and training programme for internal control monitoring is defined. A process is defined for self-assessments and internal control assurance reviews, with roles for responsible business and IT managers. Tools are being utilised but are not necessarily integrated into all processes. IT process risk assessment policies are being used within control frameworks developed specifically for the IT organisation. Process-specific risks and mitigation policies are defined.

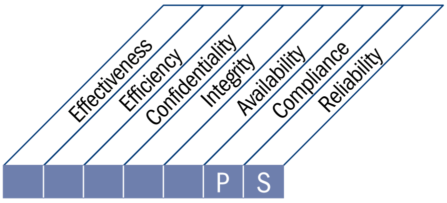
4 Managed and Measurable when
Management implements a framework for IT internal control monitoring. The organisation establishes tolerance levels for the internal control monitoring process. Tools are implemented to standardise assessments and automatically detect control exceptions. A formal IT internal control function is established, with specialised and certified professionals utilising a formal control framework endorsed by senior management. Skilled IT staff members are routinely participating in internal control assessments. A metrics knowledge base for historical information on internal control monitoring is established. Peer reviews for internal control monitoring are established.

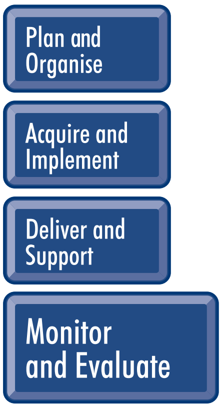
5 Optimised when
Management establishes an organisationwide continuous improvement programme that takes into account lessons learned and industry good practices for internal control monitoring. The organisation uses integrated and updated tools, where appropriate, that allow effective assessment of critical IT controls and rapid detection of IT control monitoring incidents. Knowledge sharing specific to the information services function is formally implemented. Benchmarking against industry standards and good practices is formalised.

Process Description

ME3 Ensure Compliance With External Requirements

Effective oversight of compliance requires the establishment of a review process to ensure compliance with laws, regulations and contractual requirements. This process includes identifying compliance requirements, optimising and evaluating the response, obtaining assurance that the requirements have been complied with and, finally, integrating IT's compliance reporting with the rest of the business.





Control over the IT process of

Ensure compliance with external requirements

that satisfies the business requirement for IT of

ensuring compliance with laws, regulations and contractual requirements

by focusing on

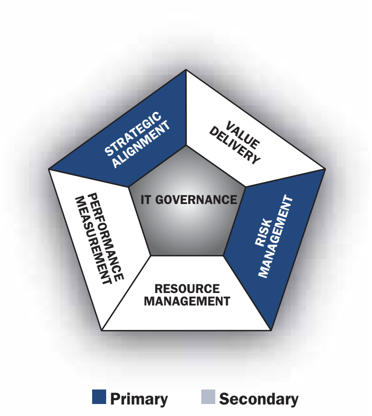
identifying all applicable laws, regulations and contracts and the corresponding level of IT compliance and optimising IT processes to reduce the risk of non-compliance

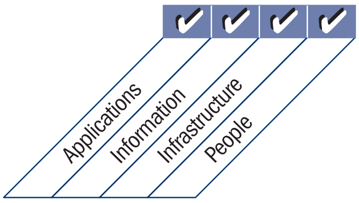
is achieved by

- Identifying legal, regulatory and contractual requirements related to IT
- Assessing the impact of compliance requirements
- Monitoring and reporting on compliance with these requirements

and is measured by

- Cost of IT non-compliance, including settlements and fines
- Average time lag between identification of external compliance issues and resolution
- Frequency of compliance reviews





Control Objectives

ME3 Ensure Compliance With External Requirements

ME3.1 Identification of External Legal, Regulatory and Contractual Compliance Requirements
Identify, on a continuous basis, local and international laws, regulations, and other external requirements that must be complied with for incorporation into the organisation's IT policies, standards, procedures and methodologies.

ME3.2 Optimisation of Response to External Requirements
Review and adjust IT policies, standards, procedures and methodologies to ensure that legal, regulatory and contractual requirements are addressed and communicated.

ME3.3 Evaluation of Compliance With External Requirements
Confirm compliance of IT policies, standards, procedures and methodologies with legal and regulatory requirements.

ME3.4 Positive Assurance of Compliance
Obtain and report assurance of compliance and adherence to all internal policies derived from internal directives or external legal, regulatory or contractual requirements, confirming that any corrective actions to address any compliance gaps have been taken by the responsible process owner in a timely manner.

ME3.5 Integrated Reporting
Integrate IT reporting on legal, regulatory and contractual requirements with similar output from other business functions.

Management Guidelines

ME3 Ensure Compliance With External Requirements

From	Inputs
*	Legal and regulatory compliance requirements
PO6	IT policies

* Input from outside COBIT

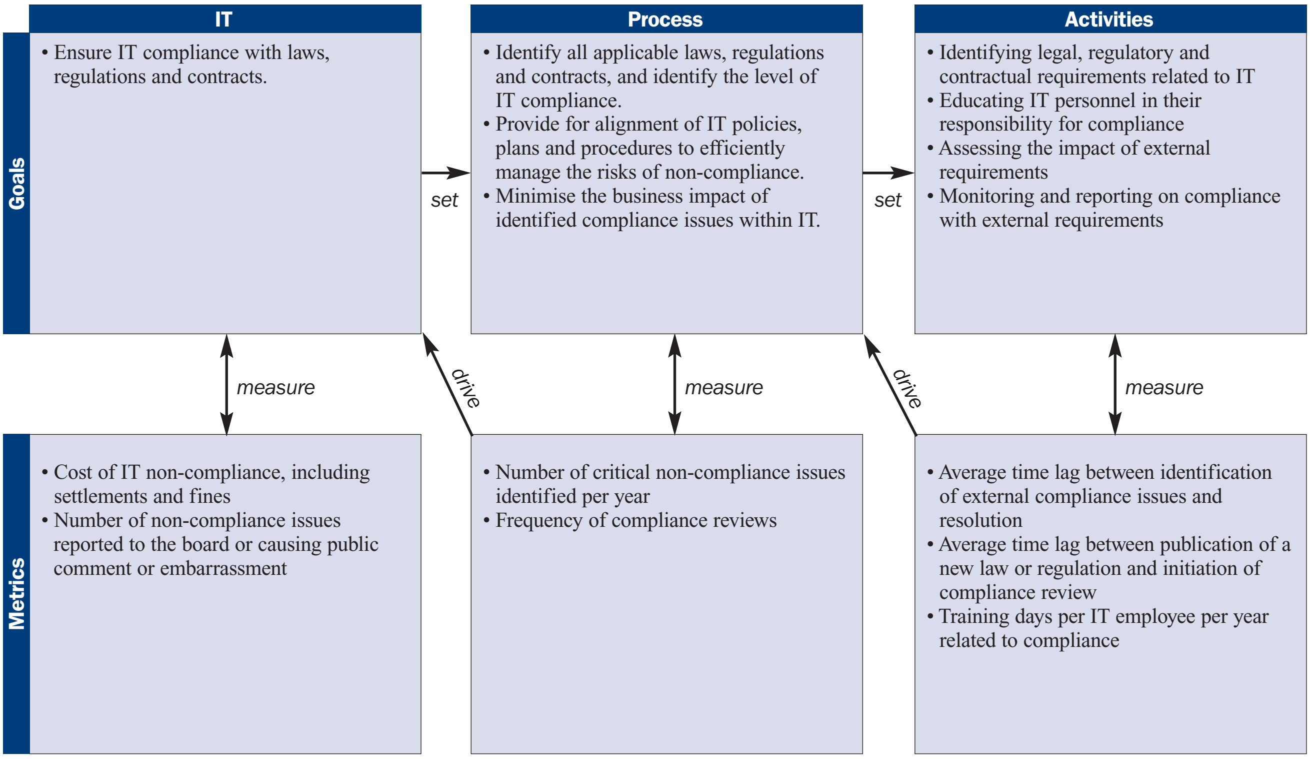
Outputs	To						
Catalogue of legal and regulatory requirements related to IT service delivery	PO4	ME4					
Report on compliance of IT activities with external legal and regulatory requirements	ME1						

RACI Chart

Activities	CEO	CFO	Business Executive	CIO	Business Process Owner	Head Operations	Chief Architect	Head Development	Head IT Administration	PMO	Compliance, Audit, Risk and Security	Board
Define and execute a process to identify legal, contractual, policy and regulatory requirements.				A/R	C	I	I	I	C	I	R	
Evaluate compliance of IT activities with IT policies, plans and procedures.	I	I	I	A/R	I	R	R	R	R	R	R	I
Report positive assurance of compliance of IT activities with IT policies, plans and procedures.				A/R	C	C	C	C	C	C	R	
Provide input to align IT policies, plans and procedures in response to compliance requirements.				A/R	C	C	C	C	C		R	
Integrate IT reporting on regulatory requirements with similar output from other business functions.				A/R		I	I	I	R	I	R	

A **RACI** chart identifies who is **R**esponsible, **A**ccountable, **C**onsulted and/or **I**nformed.

Goals and Metrics



IT

Goals:
- Ensure IT compliance with laws, regulations and contracts.

Metrics:
- Cost of IT non-compliance, including settlements and fines
- Number of non-compliance issues reported to the board or causing public comment or embarrassment

Process

Goals:
- Identify all applicable laws, regulations and contracts, and identify the level of IT compliance.
- Provide for alignment of IT policies, plans and procedures to efficiently manage the risks of non-compliance.
- Minimise the business impact of identified compliance issues within IT.

Metrics:
- Number of critical non-compliance issues identified per year
- Frequency of compliance reviews

Activities

Goals:
- Identifying legal, regulatory and contractual requirements related to IT
- Educating IT personnel in their responsibility for compliance
- Assessing the impact of external requirements
- Monitoring and reporting on compliance with external requirements

Metrics:
- Average time lag between identification of external compliance issues and resolution
- Average time lag between publication of a new law or regulation and initiation of compliance review
- Training days per IT employee per year related to compliance

Maturity Model

ME3 Ensure Compliance With External Requirements

Management of the process of *Ensure compliance with external requirements* that satisfies the business requirement for IT of *ensuring compliance with laws, regulations and contractual requirements* is:

0 Non-existent when
There is little awareness of external requirements that affect IT, with no process regarding compliance with regulatory, legal and contractual requirements.

1 Initial/*Ad Hoc* when
There is awareness of regulatory, contractual and legal compliance requirements impacting the organisation. Informal processes are followed to maintain compliance, but only as the need arises in new projects or in response to audits or reviews.

2 Repeatable but Intuitive when
There is an understanding of the need to comply with external requirements, and the need is communicated. Where compliance is a recurring requirement, as in financial regulations or privacy legislation, individual compliance procedures have been developed and are followed on a year-to-year basis. There is, however, no standard approach. There is high reliance on the knowledge and responsibility of individuals, and errors are likely. There is informal training regarding external requirements and compliance issues.

3 Defined when
Policies, plans and procedures are developed, documented and communicated to ensure compliance with regulations and contractual and legal obligations, but some may not always be followed, and some may be out of date or impractical to implement. There is little monitoring performed and there are compliance requirements that have not been addressed. Training is provided in external legal and regulatory requirements affecting the organisation and the defined compliance processes. Standard *pro forma* contracts and legal processes exist to minimise the risks associated with contractual liability.

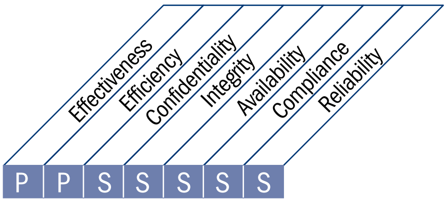
4 Managed and Measurable when
Issues and exposures from external requirements and the need to ensure compliance at all levels are fully understood. A formal training scheme is in place to ensure that all staff members are aware of their compliance obligations. Responsibilities are clear and process ownership is understood. The process includes a review of the environment to identify external requirements and ongoing changes. There is a mechanism in place to monitor non-compliance with external requirements, enforce internal practices and implement corrective action. Non-compliance issues are analysed for root causes in a standard manner, with the objective to identify sustainable solutions. Standardised internal good practices are utilised for specific needs, such as standing regulations and recurring service contracts.

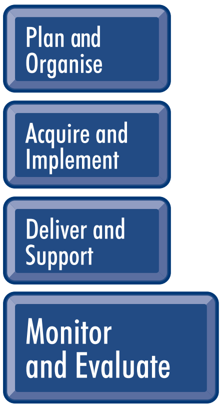
5 Optimised when
A well-organised, efficient and enforced process is in place for complying with external requirements, based on a single central function that provides guidance and co-ordination to the whole organisation. Extensive knowledge of the applicable external requirements, including their future trends and anticipated changes, and the need for new solutions exist. The organisation takes part in external discussions with regulatory and industry groups to understand and influence external requirements affecting them. Good practices are developed ensuring efficient compliance with external requirements, resulting in very few cases of compliance exceptions. A central, organisationwide tracking system exists, enabling management to document the workflow and to measure and improve the quality and effectiveness of the compliance monitoring process. An external requirements self-assessment process is implemented and refined to a level of good practice. The organisation's management style and culture relating to compliance are sufficiently strong, and processes are developed well enough for training to be limited to new personnel and whenever there is a significant change.

Process Description

ME4 Provide IT Governance

Establishing an effective governance framework includes defining organisational structures, processes, leadership, roles and responsibilities to ensure that enterprise IT investments are aligned and delivered in accordance with enterprise strategies and objectives.





Control over the IT process of

Provide IT governance

that satisfies the business requirement for IT of

integrating IT governance with corporate governance objectives and complying with laws, regulations and contracts

by focusing on

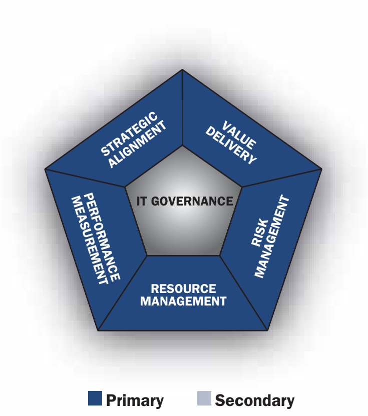
preparing board reports on IT strategy, performance and risks, and responding to governance requirements in line with board directions

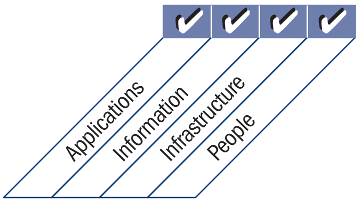
is achieved by

- Establishing an IT governance framework integrated into corporate governance
- Obtaining independent assurance over the IT governance status

and is measured by

- Frequency of board reporting on IT to stakeholders (including maturity)
- Frequency of reporting from IT to the board (including maturity)
- Frequency of independent reviews of IT compliance





Control Objectives

ME4 Provide IT Governance

ME4.1 Establishment of an IT Governance Framework
Define, establish and align the IT governance framework with the overall enterprise governance and control environment. Base the framework on a suitable IT process and control model and provide for unambiguous accountability and practices to avoid a breakdown in internal control and oversight. Confirm that the IT governance framework ensures compliance with laws and regulations and is aligned with, and confirms delivery of, the enterprise's strategies and objectives. Report IT governance status and issues.

ME4.2 Strategic Alignment
Enable board and executive understanding of strategic IT issues, such as the role of IT, technology insights and capabilities. Ensure that there is a shared understanding between the business and IT regarding the potential contribution of IT to the business strategy. Work with the board and the established governance bodies, such as an IT strategy committee, to provide strategic direction to management relative to IT, ensuring that the strategy and objectives are cascaded into business units and IT functions, and that confidence and trust are developed between the business and IT. Enable the alignment of IT to the business in strategy and operations, encouraging co-responsibility between the business and IT for making strategic decisions and obtaining benefits from IT-enabled investments.

ME4.3 Value Delivery
Manage IT-enabled investment programmes and other IT assets and services to ensure that they deliver the greatest possible value in supporting the enterprise's strategy and objectives. Ensure that the expected business outcomes of IT-enabled investments and the full scope of effort required to achieve those outcomes are understood; that comprehensive and consistent business cases are created and approved by stakeholders; that assets and investments are managed throughout their economic life cycle; and that there is active management of the realisation of benefits, such as contribution to new services, efficiency gains and improved responsiveness to customer demands. Enforce a disciplined approach to portfolio, programme and project management, insisting that the business takes ownership of all IT-enabled investments and IT ensures optimisation of the costs of delivering IT capabilities and services.

ME4.4 Resource Management
Oversee the investment, use and allocation of IT resources through regular assessments of IT initiatives and operations to ensure appropriate resourcing and alignment with current and future strategic objectives and business imperatives.

ME4.5 Risk Management
Work with the board to define the enterprise's appetite for IT risk, and obtain reasonable assurance that IT risk management practices are appropriate to ensure that the actual IT risk does not exceed the board's risk appetite. Embed risk management responsibilities into the organisation, ensuring that the business and IT regularly assess and report IT-related risks and their impact and that the enterprise's IT risk position is transparent to all stakeholders.

ME4.6 Performance Measurement
Confirm that agreed-upon IT objectives have been met or exceeded, or that progress toward IT goals meets expectations. Where agreed-upon objectives have been missed or progress is not as expected, review management's remedial action. Report to the board relevant portfolios, programme and IT performance, supported by reports to enable senior management to review the enterprise's progress toward identified goals.

ME4.7 Independent Assurance
Obtain independent assurance (internal or external) about the conformance of IT with relevant laws and regulations; the organisation's policies, standards and procedures; generally accepted practices; and the effective and efficient performance of IT.

Management Guidelines

ME4 Provide IT Governance

From	Inputs
PO4	IT process framework
PO5	Cost-benefit reports
PO9	Risk assessment and reporting
ME2	Report on effectiveness of IT controls
ME3	Catalogue of legal and regulatory requirements related to IT service delivery

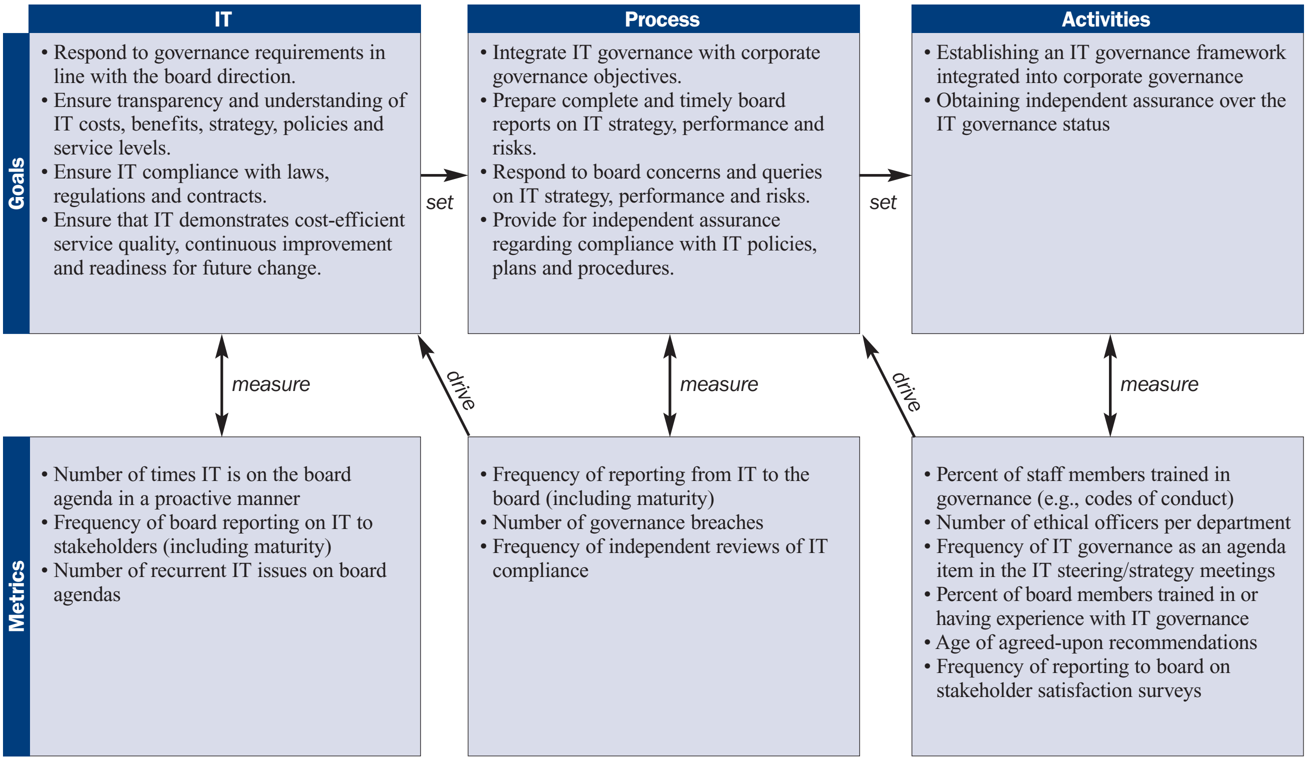
Outputs	To						
Process framework improvements	PO4						
Report on IT governance status	PO1	ME1					
Expected business outcome of IT-enabled business investments	PO5						
Enterprise strategic direction for IT	PO1						
Enterprise appetite for IT risks	PO9						

RACI Chart

Activities \ Functions	Board	CEO	CFO	Business Executive	CIO	Business Process Owner	Head Operations	Chief Architect	Head Development	Head IT Administration	PMO	Compliance, Audit, Risk and Security
Establish executive and board oversight and facilitation over IT activities.	A	R	C	C	C							C
Review, endorse, align and communicate IT performance, IT strategy, and resource and risk management with business strategy.	A	R	I	I	R							C
Obtain periodic independent assessment of performance and compliance with policies, plans and procedures.	A	R	C	I	C		I	I	I	I	I	R
Resolve findings of independent assessments, and ensure management's implementation of agreed-upon recommendations.	A	R	C	I	C		I	I	I	I	I	R
Generate an IT governance report.	A	C	C	C	R	C	I	I	I	I	I	C

A **RACI** chart identifies who is **R**esponsible, **A**ccountable, **C**onsulted and/or **I**nformed.

Goals and Metrics



	IT	Process	Activities
Goals	• Respond to governance requirements in line with the board direction. • Ensure transparency and understanding of IT costs, benefits, strategy, policies and service levels. • Ensure IT compliance with laws, regulations and contracts. • Ensure that IT demonstrates cost-efficient service quality, continuous improvement and readiness for future change.	• Integrate IT governance with corporate governance objectives. • Prepare complete and timely board reports on IT strategy, performance and risks. • Respond to board concerns and queries on IT strategy, performance and risks. • Provide for independent assurance regarding compliance with IT policies, plans and procedures.	• Establishing an IT governance framework integrated into corporate governance • Obtaining independent assurance over the IT governance status
Metrics	• Number of times IT is on the board agenda in a proactive manner • Frequency of board reporting on IT to stakeholders (including maturity) • Number of recurrent IT issues on board agendas	• Frequency of reporting from IT to the board (including maturity) • Number of governance breaches • Frequency of independent reviews of IT compliance	• Percent of staff members trained in governance (e.g., codes of conduct) • Number of ethical officers per department • Frequency of IT governance as an agenda item in the IT steering/strategy meetings • Percent of board members trained in or having experience with IT governance • Age of agreed-upon recommendations • Frequency of reporting to board on stakeholder satisfaction surveys

Maturity Model

ME4 Provide IT Governance

Management of the process of *Provide IT governance* that satisfies the business requirement for IT of *integrating IT governance with corporate governance objectives and complying with laws and regulations* is:

0 Non-existent when
There is a complete lack of any recognisable IT governance process. The organisation does not even recognise that there is an issue to be addressed; hence, there is no communication about the issue.

1 Initial/*Ad Hoc* when
There is recognition that IT governance issues exist and need to be addressed. There are *ad hoc* approaches applied on an individual or case-by-case basis. Management's approach is reactive, and there is only sporadic, inconsistent communication on issues and approaches to address them. Management has only an approximate indication of how IT contributes to business performance. Management only reactively responds to an incident that has caused some loss or embarrassment to the organisation.

2 Repeatable but Intuitive when
There is awareness of IT governance issues. IT governance activities and performance indicators, which include IT planning, delivery and monitoring processes, are under development. Selected IT processes are identified for improvement based on individuals' decisions. Management identifies basic IT governance measurements and assessment methods and techniques; however, the process is not adopted across the organisation. Communication on governance standards and responsibilities is left to the individual. Individuals drive the governance processes within various IT projects and processes. The processes, tools and metrics to measure IT governance are limited and may not be used to their full capacity due to a lack of expertise in their functionality.

3 Defined when
The importance of and need for IT governance are understood by management and communicated to the organisation. A baseline set of IT governance indicators is developed where linkages between outcome measures and performance indicators are defined and documented. Procedures are standardised and documented. Management communicates standardised procedures, and training is established. Tools are identified to assist with overseeing IT governance. Dashboards are defined as part of the IT balanced business scorecard. However, it is left to the individual to get training, follow the standards and apply them. Processes may be monitored, but deviations, while mostly being acted upon by individual initiative, are unlikely to be detected by management.

4 Managed and Measurable when
There is full understanding of IT governance issues at all levels. There is a clear understanding of who the customer is, and responsibilities are defined and monitored through SLAs. Responsibilities are clear and process ownership is established. IT processes and IT governance are aligned with and integrated into the business and the IT strategy. Improvement in IT processes is based primarily upon a quantitative understanding, and it is possible to monitor and measure compliance with procedures and process metrics. All process stakeholders are aware of risks, the importance of IT and the opportunities it can offer. Management defines tolerances under which processes must operate. There is limited, primarily tactical, use of technology, based on mature techniques and enforced standard tools. IT governance has been integrated into strategic and operational planning and monitoring processes. Performance indicators over all IT governance activities are being recorded and tracked, leading to enterprisewide improvements. Overall accountability of key process performance is clear, and management is rewarded based on key performance measures.

5 Optimised when
There is an advanced and forward-looking understanding of IT governance issues and solutions. Training and communication are supported by leading-edge concepts and techniques. Processes are refined to a level of industry good practice, based on results of continuous improvement and maturity modelling with other organisations. The implementation of IT policies leads to an organisation, people and processes that are quick to adapt and fully support IT governance requirements. All problems and deviations are root cause analysed, and efficient action is expediently identified and initiated. IT is used in an extensive, integrated and optimised manner to automate the workflow and provide tools to improve quality and effectiveness. The risks and returns of the IT processes are defined, balanced and communicated across the enterprise. External experts are leveraged and benchmarks are used for guidance. Monitoring, self-assessment and communication about governance expectations are pervasive within the organisation, and there is optimal use of technology to support measurement, analysis, communication and training. Enterprise governance and IT governance are strategically linked, leveraging technology and human and financial resources to increase the competitive advantage of the enterprise. IT governance activities are integrated with the enterprise governance process.

APPENDIX I

TABLES LINKING GOALS AND PROCESSES

This appendix provides a global view of how generic business goals relate to IT goals, the IT processes and information criteria. There are three tables:

1. The first table maps the business goals, organised according to a balanced scorecard, to the IT goals and information criteria. This helps show, for a given generic business goal, the IT goals that typically support this goal and the COBIT information criteria that relate to the business goal. The set of 17 business goals should not be regarded as a complete set of all possible business goals; it is a selection of relevant business goals that can have a clear impact on IT (IT-related business goals).
2. The second table maps the IT goals to COBIT's IT processes and the information criteria on which the IT goal is based.
3. The third table provides a reverse mapping showing for each IT process the IT goals that are supported.

The tables help demonstrate the scope of COBIT and the overall business relationship between COBIT and business drivers, enabling typical IT-related business goals to be mapped via IT goals to the IT processes needed to support them. The tables are based on generic goals and, therefore, should be used as a guide and tailored for a specific enterprise.

To provide a link back to the information criteria used for business requirements in COBIT 3rd Edition, the tables also provide an indication of the most important information criteria supported by the business and IT goals.

Notes:

1. The information criteria in the business goals chart are based on an aggregation of the criteria for the related IT goals and a subjective assessment of those that are most relevant to the business goal. No attempt has been made to indicate primary or secondary. These are only indicative and users can follow a similar process when assessing their own business goals.
2. The information criteria primary and secondary references in the IT goals chart are based on an aggregation of the criteria for each IT process and a subjective assessment of what is primary and secondary for the IT goal, as some processes have more of an impact on the IT goal than others. These are only indicative and users can follow a similar process when assessing their own IT goals.

APPENDIX I—TABLES LINKING GOALS AND PROCESSES

LINKING BUSINESS GOALS TO IT GOALS

											COBIT Information Criteria						
		Business Goals	**IT Goals**								Effectiveness	Efficiency	Confidentiality	Integrity	Availability	Compliance	Reliability
Financial Perspective	**1**	Provide a good return on investment of IT-enabled business investments.	24														
	2	Manage IT-related business risk.	2	14	17	18	19	20	21	22							
	3	Improve corporate governance and transparency.	2	18													
Customer Perspective	**4**	Improve customer orientation and service.	3	23													
	5	Offer competitive products and services.	5	24													
	6	Establish service continuity and availability.	10	16	22	23											
	7	Create agility in responding to changing business requirements.	1	5	25												
	8	Achieve cost optimisation of service delivery.	7	8	10	24											
	9	Obtain reliable and useful information for strategic decision making.	2	4	12	20	26										
Internal Perspective	**10**	Improve and maintain business process functionality.	6	7	11												
	11	Lower process costs.	7	8	13	15	24										
	12	Provide compliance with external laws, regulations and contracts.	2	19	20	21	22	26	27								
	13	Provide compliance with internal policies.	2	13													
	14	Manage business change.	1	5	6	11	28										
	15	Improve and maintain operational and staff productivity.	7	8	11	13											
Learning and Growth Perspective	**16**	Manage product and business innovation.	5	25	28												
	17	Acquire and maintain skilled and motivated people.	9														

LINKING IT GOALS TO IT PROCESSES

	IT Goals	Processes											COBIT Information Criteria						
													Effectiveness	Efficiency	Confidentiality	Integrity	Availability	Compliance	Reliability
1	Respond to business requirements in alignment with the business strategy.	PO1	PO2	PO4	PO10	AI1	AI6	AI7	DS1	DS3	ME1		P	P		S	S		
2	Respond to governance requirements in line with board direction.	PO1	PO4	PO10	ME1	ME4							P	P					
3	Ensure satisfaction of end users with service offerings and service levels.	PO8	AI4	DS1	DS2	DS7	DS8	DS10	DS13				P	P		S	S		
4	Optimise the use of information.	PO2	DS11											S		P			S
5	Create IT agility.	PO2	PO4	PO7	AI3								P	P		S			
6	Define how business functional and control requirements are translated in effective and efficient automated solutions.	AI1	AI2	AI6									P	P				S	
7	Acquire and maintain integrated and standardised application systems.	PO3	AI2	AI5									P	P				S	
8	Acquire and maintain an integrated and standardised IT infrastructure.	AI3	AI5										S	P					
9	Acquire and maintain IT skills that respond to the IT strategy.	PO7	AI5										P	P					
10	Ensure mutual satisfaction of third-party relationships.	DS2											P	P	S	S	S	S	S
11	Ensure seamless integration of applications into business processes.	PO2	AI4	AI7									P	P		S	S		
12	Ensure transparency and understanding of IT cost, benefits, strategy, policies and service levels.	PO5	PO6	DS1	DS2	DS6	ME1	ME4					P	P				S	S
13	Ensure proper use and performance of the applications and technology solutions.	PO6	AI4	AI7	DS7	DS8							P	S					
14	Account for and protect all IT assets.	PO9	DS5	DS9	DS12	ME2							S	S	P	P	P	S	S
15	Optimise the IT infrastructure, resources and capabilities.	PO3	AI3	DS3	DS7	DS9							S	P					
16	Reduce solution and service delivery defects and rework.	PO8	AI4	AI6	AI7	DS10							P	P		S	S		
17	Protect the achievement of IT objectives.	PO9	DS10	ME2									P	P	S	S	S	S	S
18	Establish clarity of business impact of risks to IT objectives and resources.	PO9											S	S	P	P	P	S	S
19	Ensure that critical and confidential information is withheld from those who should not have access to it.	PO6	DS5	DS11	DS12										P	P	S	S	S
20	Ensure that automated business transactions and information exchanges can be trusted.	PO6	AI7	DS5									P			P	S	S	
21	Ensure that IT services and infrastructure can properly resist and recover from failures due to error, deliberate attack or disaster.	PO6	AI7	DS4	DS5	DS12	DS13	ME2					P	S		S	P		
22	Ensure minimum business impact in the event of an IT service disruption or change.	PO6	AI6	DS4	DS12								P	S		S	P		
23	Make sure that IT services are available as required.	DS3	DS4	DS8	DS13								P	P			P		
24	Improve IT's cost-efficiency and its contribution to business profitability.	PO5	DS6										S	P					S
25	Deliver projects on time and on budget, meeting quality standards.	PO8	PO10										P	P		S			S
26	Maintain the integrity of information and processing infrastructure.	AI6	DS5										P	P		P	P		S
27	Ensure IT compliance with laws, regulations and contracts.	DS11	ME2	ME3	ME4										S	S		P	S
28	Ensure that IT demonstrates cost-efficient service quality, continuous improvement and readiness for future change.	PO5	DS6	ME1	ME4								P	P					P

IT PROCESS TO IT GOALS MATRIX

	Respond to business requirements in alignment with the business strategy.	Respond to governance requirements in line with board direction.	Ensure satisfaction of end users with service offerings and service levels.	Optimise use of information.	Create IT agility.	Define how business functional and control requirements are translated in effective and efficient automated solutions.	Acquire and maintain integrated and standardised application systems.	Acquire and maintain an integrated and standardised IT infrastructure.	Acquire and maintain IT skills that respond to the IT strategy.	Ensure mutual satisfaction of third-party relationships.	Ensure seamless integratation of applications into business processes.	Ensure transparency and understanding of IT cost, benefits, strategy, policies and service levels.	Ensure proper use and performance of the applications and technology solutions.	Account for and protect all IT assets.	Optimise the IT infrastructure, resources and capabilities.	Reduce solution and service delivery defects and rework.	Protect the achievement of IT objectives.	Establish clarity on the business impact of risks to IT objectives and resources.	Ensure that critical and confidential information is withheld from those who should not have access to it.	Ensure that automated business transactions and information exchanges can be trusted.	Ensure that IT services and infrastructure can properly resist and recover from failures due to error, deliberate attack or disaster.	Ensure minimum business impact in the event of an IT service disruption or change.	Make sure that IT services are available as required.	Improve IT's cost-efficiency and its contribution to business profitability.	Deliver projects on time and on budget, meeting quality standards.	Maintain the integrity of information and processing infrastructure.	Ensure IT compliance with laws, regulations and contracts.	Ensure that IT demonstrates cost-efficient service quality, continuous improvement and readiness for future change.
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
Plan and Organise																												
PO1 Define a strategic IT plan.	✔	✔																										
PO2 Define the information architecture.	✔			✔	✔						✔																	
PO3 Determine technological direction.							✔								✔													
PO4 Define the IT processes, organisation and relationships.	✔	✔			✔																							
PO5 Manage the IT investment.												✔												✔				✔
PO6 Communicate management aims and direction.												✔	✔						✔	✔	✔	✔						
PO7 Manage IT human resources.					✔				✔																			
PO8 Manage quality.			✔													✔									✔			
PO9 Assess and manage IT risks.														✔			✔	✔										
PO10 Manage projects.	✔	✔																							✔			
Acquire and Implement																												
AI1 Identify automated solutions.	✔					✔																						
AI2 Acquire and maintain application software.						✔	✔																					
AI3 Acquire and maintain technology infrastructure.					✔			✔							✔													
AI4 Enable operation and use.			✔								✔		✔			✔												
AI5 Procure IT resources.							✔	✔	✔																			
AI6 Manage changes.	✔					✔										✔						✔				✔		
AI7 Install and accredit solutions and changes.	✔										✔		✔			✔				✔	✔							
Deliver and Support																												
DS1 Define and manage service levels.	✔		✔									✔																
DS2 Manage third-party services.			✔							✔		✔																
DS3 Manage performance and capacity.	✔														✔								✔					
DS4 Ensure continuous service.																					✔	✔	✔					
DS5 Ensure systems security.														✔					✔	✔	✔					✔		
DS6 Identify and allocate costs.												✔												✔				✔
DS7 Educate and train users.			✔										✔		✔													
DS8 Manage service desk and incidents.			✔										✔										✔					
DS9 Manage the configuration.														✔	✔													
DS10 Manage problems.			✔													✔	✔											
DS11 Manage data.				✔															✔								✔	
DS12 Manage the physical environment.														✔					✔		✔	✔						
DS13 Manage operations.			✔																		✔		✔					
Monitor and Evaluate																												
ME1 Monitor and evaluate IT performance.	✔	✔										✔																✔
ME2 Monitor and evaluate internal control.														✔			✔				✔						✔	
ME3 Ensure compliance with external requirements.																											✔	
ME4 Provide IT governance.		✔										✔															✔	✔

Appendix II

Mapping IT Processes to IT Governance Focus Areas, COSO, CobiT IT Resources and CobiT Information Criteria

This appendix provides a mapping between the CobiT IT processes and the five IT governance focus areas, the components of COSO, IT resources and the information criteria. The table also provides a relative importance indicator (high, medium and low) based on benchmarking via CobiT Online. This matrix demonstrates on one page and at a high level how the CobiT framework addresses IT governance and COSO requirements, and shows the relationship between IT processes and the IT resources and information criteria. P is used when there is a primary relation and S when there is only a secondary relation. No P or S does not mean that there is no relation, only that it is less important, or marginal. The importance values are based on a survey and the opinions of experts, and are provided only as a guide. Users should consider what processes are important within their own organisations.

APPENDIX II—MAPPING IT PROCESSES TO IT GOVERNANCE FOCUS AREAS, COSO, COBIT IT RESOURCES AND COBIT INFORMATION CRITERIA

		IT Governance Focus Areas					COSO					COBIT IT Resources				COBIT Information Criteria						
	IMPORTANCE	Strategic Alignment	Value Delivery	Resource Management	Risk Management	Performance Measurement	Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring	Application	Information	Infrastructure	People	Effectiveness	Efficiency	Confidentiality	Integrity	Availability	Compliance	Reliability
Plan and Organise																						
P01 Define a strategic IT plan.	H	P		S	S			P		S	S					P	S					
P02 Define the information architecture.	L	P	S	P	S				P	P						S	P	S	P			
P03 Determine technological direction.	M	S	S	P	S			S	P	S						P	P					
P04 Define the IT processes, organisation and relationships.	L	S		P	P		P			S	S					P	P					
P05 Manage the IT investment.	M	S	P	S		S		S	P							P	P					S
P06 Communicate management aims and direction.	M	P			P		P			P						P					S	
P07 Manage IT human resources.	L	P		P	S	S	P			S						P	P					
P08 Manage quality.	M	P	S		S		P		P	S	P					P	P		S			S
P09 Assess and manage IT risks.	H	P			P			P								S	S	P	P	P	S	S
P010 Manage projects.	H	P	S	S	S	S	S	S	P		S					P	P					
Acquire and Implement																						
AI1 Identify automated solutions.	M	P	P	S	S				P							P	S					
AI2 Acquire and maintain application software.	M	P	P		S				P							P	P		S			S
AI3 Acquire and maintain technology infrastructure.	L			P					P							S	P		S	S		
AI4 Enable operation and use.	L	S	P	S	S				P	S						P	P		S	S	S	S
AI5 Procure IT resources.	M		S	P					P							S	P				S	
AI6 Manage changes.	H		P	S				S	P		S					P	P		P	P		S
AI7 Install and accredit solutions and changes.	M	S	P	S	S	S			P	S	S					P	S		S	S		
Deliver and Support																						
DS1 Define and manage service levels.	M	P	P	P		P	S		P	S	S					P	P	S	S	S	S	S
DS2 Manage third-party services.	L		P	S	P	S	P	S	P		S					P	P	S	S	S	S	S
DS3 Manage performance and capacity.	L	S	S	P	S	S			P		S					P	P			S		
DS4 Ensure continuous service.	M	S	P	S	P	S	S		P	S						P	S			P		
DS5 Ensure systems security.	H				P				P	S	S							P	P	S	S	S
DS6 Identify and allocate costs.	L		S	P		S			P								P					P
DS7 Educate and train users.	L	S	P	S	S		P			S						P	S					
DS8 Manage service desk and incidents.	L		P			S	S			P	P					P	P					
DS9 Manage the configuration.	M		P	P	S				P							P	S			S		S
DS10 Manage problems.	M		P		S	S			P	S	S					P	P			S		
DS11 Manage data.	H		P	P	P				P										P			P
DS12 Manage the physical environment.	L			S	P			S	P										P	P		
DS13 Manage operations.	L			P					P	S						P	P		S	S		
Monitor and Evaluate																						
ME1 Monitor and evaluate IT performance.	H	S	S	S	S	P				S	P					P	P	S	S	S	S	S
ME2 Monitor and evaluate internal control.	M		P		P						P					P	P	S	S	S	S	S
ME3 Ensure compliance with external requirements.	H	P			P				P	S	S										P	S
ME4 Provide IT governance.	H	P	P	P	P	P	P	S		S	P					P	P	S	S	S	S	S

Note: The COSO mapping is based on the original COSO framework. The mapping also applies generally to the later COSO *Enterprise Risk Management—Integrated Framework*, which expands on internal control, providing a more robust and extensive focus on the broader subject of enterprise risk management. Whilst it is not intended to and does not replace the original COSO internal control framework, but rather incorporates the internal control framework within it, users of CobiT may choose to refer to this enterprise risk management framework both to satisfy their internal control needs and to move toward a fuller risk management process.

Page intentionally left blank

Appendix III

Maturity Model for Internal Control

This appendix provides a generic maturity model showing the status of the internal control environment and the establishment of internal controls in an enterprise. It shows how the management of internal control, and an awareness of the need to establish better internal controls, typically develops from an *ad hoc* to an optimised level. The model provides a high-level guide to help COBIT users appreciate what is required for effective internal controls in IT and to help position their enterprise on the maturity scale.

APPENDIX III—MATURITY MODEL FOR INTERNAL CONTROL

Maturity Level	Status of the Internal Control Environment	Establishment of Internal Controls
0 Non-existent	There is no recognition of the need for internal control. Control is not part of the organisation's culture or mission. There is a high risk of control deficiencies and incidents.	There is no intent to assess the need for internal control. Incidents are dealt with as they arise.
1 Initial/*ad hoc*	There is some recognition of the need for internal control. The approach to risk and control requirements is *ad hoc* and disorganised, without communication or monitoring. Deficiencies are not identified. Employees are not aware of their responsibilities.	There is no awareness of the need for assessment of what is needed in terms of IT controls. When performed, it is only on an *ad hoc* basis, at a high level and in reaction to significant incidents. Assessment addresses only the actual incident.
2 Repeatable but intuitive	Controls are in place but are not documented. Their operation is dependent on knowledge and motivation of individuals. Effectiveness is not adequately evaluated. Many control weaknesses exist and are not adequately addressed; the impact can be severe. Management actions to resolve control issues are not prioritised or consistent. Employees may not be aware of their responsibilities.	Assessment of control needs occurs only when needed for selected IT processes to determine the current level of control maturity, the target level that should be reached and the gaps that exist. An informal workshop approach, involving IT managers and the team involved in the process, is used to define an adequate approach to controls for the process and to motivate an agreed-upon action plan.
3 Defined	Controls are in place and are adequately documented. Operating effectiveness is evaluated on a periodic basis and there is an average number of issues. However, the evaluation process is not documented. Whilst management is able to deal predictably with most control issues, some control weaknesses persist and impacts could still be severe. Employees are aware of their responsibilties for control.	Critical IT processes are identified based on value and risk drivers. A detailed analysis is performed to identify control requirements and the root cause of gaps and to develop improvement opportunities. In addition to facilitated workshops, tools are used and interviews are performed to support the analysis and ensure that an IT process owner owns and drives the assessment and improvement process.
4 Managed and measurable	There is an effective internal control and risk management environment. A formal, documented evaluation of controls occurs frequently. Many controls are automated and regularly reviewed. Management is likely to detect most control issues, but not all issues are routinely identified. There is consistent follow-up to address identified control weaknesses. A limited, tactical use of technology is applied to automate controls.	IT process criticality is regularly defined with full support and agreement from the relevant business process owners. Assessment of control requirements is based on policy and the actual maturity of these processes, following a thorough and measured analysis involving key stakeholders. Accountability for these assessments is clear and enforced. Improvement strategies are supported by business cases. Performance in achieving the desired outcomes is consistently monitored. External control reviews are organised occasionally.
5 Optimised	An enterprisewide risk and control programme provides continuous and effective control and risk issues resolution. Internal control and risk management are integrated with enterprise practices, supported with automated real-time monitoring with full accountability for control monitoring, risk management and compliance enforcement. Control evaluation is continuous, based on self-assessments and gap and root cause analyses. Employees are proactively involved in control improvements.	Business changes consider the criticality of IT processes, and cover any need to reassess process control capability. IT process owners regularly perform self-assessments to confirm that controls are at the right level of maturity to meet business needs and they consider maturity attributes to find ways to make controls more efficient and effective. The organisation benchmarks to external good practices and seeks external advice on internal control effectiveness. For critical processes, independent reviews take place to provide assurance that the controls are at the desired level of maturity and working as planned.

Page intentionally left blank

Appendix IV

CobiT 4.1 Primary Reference Material

Appendix IV
Reference
Material

APPENDIX IV—COBIT 4.1 PRIMARY REFERENCE MATERIAL

For the earlier COBIT development and updating activities, a broad base of more than 40 international detailed IT standards, frameworks, guidelines and good practices was used to ensure the completeness of COBIT in addressing all areas of IT governance and control.

Because COBIT is focused on *what* is required to achieve adequate management and control of IT, it is positioned at a high level. The more detailed IT standards and good practices are at a lower level of detail describing *how* to manage and control specific aspects of IT. COBIT acts as an integrator of these different guidance materials, summarising key objectives under one umbrella framework that also links to governance and business requirements.

For this COBIT update (COBIT 4.1), six of the major global IT-related standards, frameworks and practices were focused on as the major supporting references to ensure appropriate coverage, consistency and alignment. These are:

- COSO:
  Internal Control—Integrated Framework, 1994
  Enterprise Risk Management—Integrated Framework, 2004
- Office of Government Commerce (OGC®):
  IT Infrastructure Library® (ITIL®), 1999-2004
- International Organisation for Standardisation:
  ISO/IEC 27000
- Software Engineering Institute (SEI®):
  SEI Capability Maturity Model (CMM®), 1993
  SEI Capability Maturity Model Integration (CMMI®), 2000
- Project Management Institute (PMI®):
  A Guide to the Project Management Body of Knowledge (PMBOK®), 2004
- Information Security Forum (ISF):
  The Standard of Good Practice for Information Security, 2003

Additional references used in the development of COBIT 4.1 include:

- *IT Control Objectives for Sarbanes-Oxley: The Role of IT in the Design and Implementation of Internal Control Over Financial Reporting, 2nd Edition*, IT Governance Institute, USA, 2006
- *CISA Review Manual*, ISACA, 2006

Page intentionally left blank

Appendix V

Cross-references Between CobiT 3rd Edition and Cobit 4.1

APPENDIX V—CROSS-REFERENCES BETWEEN COBIT 3RD EDITION AND COBIT 4.1

FRAMEWORK-LEVEL CHANGES

The major changes to the COBIT framework as a result of the COBIT 4.0 update were as follows:
- The M domain became ME, standing for Monitor and Evaluate.
- M3 and M4 were audit processes and not IT processes. They were removed, as they were adequately covered by a number of IT audit standards, but references were provided within the updated framework to highlight management's need for, and use of, assurance functions.
- ME3 is the process related to regulatory oversight, which was previously covered by PO8.
- ME4 covers the process of governance oversight over IT, in keeping with COBIT's purpose as an IT governance framework. By positioning that process as the last in the chain, it underscores the support that each prior process provides to the ultimate aim of implementing effective IT governance in the enterprise.
- With the removal of PO8 and the need to keep the numbering for PO9 *Assess risk* and PO10 *Manage projects* consistent with COBIT 3rd Edition, PO8 became *Manage quality*, the old PO11 process. The PO domain now has 10 processes instead of 11.
- The AI domain required two changes: the addition of a procurement process and the need to include in AI5 the aspects of release management. The latter change suggested that this should be the last process in the AI domain so it became AI7. The slot this created at AI5 was used to add the new procurement process. The AI domain now has seven processes instead of six.

COBIT 4.1, an incremental update to COBIT 4.0, includes:
- Enhanced executive overview
- Explanation of goals and metrics in the framework section
- Better definitions of the core concepts. It is important to mention that the definition of a control objective changed, shifting more toward a management practice statement.
- Improved control objectives resulting from updated control practices and Val IT development activity. Some control objectives were grouped and/or reworded to avoid overlaps and make the list of control objectives within a process more consistent. These changes resulted in the renumbering of the remaining control objectives. Some other control objectives were reworded to make them more action-oriented and consistent in wording. Specific revisions include:
  - AI5.5 and AI5.6 were combined with AI5.4
  - AI7.9, AI7.10 and AI7.11 were combined with AI7.8
  - ME3 was revised to include compliance with contractual requirements in addition to legal and regulatory requirements
- Application controls have been reworked to be more effective, based on work to support controls effectiveness assessment and reporting. This resulted in a list of six application controls replacing the 18 application controls in COBIT 4.0, with further detail provided in *COBIT Control Practices, 2nd Edition.*
- The list of business goals and IT goals in appendix I was improved, based on new insights obtained during validation research executed by the University of Antwerp Management School (Belgium).
- The pull-out has been expanded to provide a quick reference list of the COBIT processes, and the overview diagram depicting the domains has been revised to include reference to the process and application control elements of the COBIT framework.
- Improvements identified by COBIT users (COBIT 4.0 and COBIT Online) have been reviewed and incorporated as appropriate.

CONTROL OBJECTIVES

As can be seen from the above description of the framework-level changes and the work to clarify and focus the control objective content, the updating of the COBIT framework has significantly changed the control objectives within it. These components have been reduced from 215 to 210, because all generic materials are now retained only at the framework level and not repeated in each process. Also, all references to applications controls were moved to the framework and specific control objectives were aggregated into new statements. To support transitional activity in relation to control objectives, the following two sets of tables show the cross-references between the new and old control objectives.

MANAGEMENT GUIDELINES

Inputs and outputs have been added to illustrate what processes need from others and what the processes typically deliver. Activities and associated responsibilities have also been provided. Inputs and activity goals replace the critical success factors of COBIT 3rd Edition. Metrics are now based on a consistent cascade of business goals, IT goals, process goals and activity goals. The COBIT 3rd Edition metrics set has also been reviewed and enhanced to make it more representative and measurable.

Cross-reference: COBIT 3rd Edition to COBIT 4.1

COBIT 3rd Edition	COBIT 4.1
PO1 Define a strategic IT plan.	
1.1 IT as part of the organisation's long- and short-range plan	1.4
1.2 IT long-range plan	1.4
1.3 IT long-range planning—approach and structure	1.4
1.4 IT long-range plan changes	1.4
1.5 Short-range planning for the IT function	1.5
1.6 Communication of IT plans	1.4
1.7 Monitoring and evaluating of IT plans	1.3
1.8 Assessment of existing systems	1.3
PO2 Define the information architecture.	
2.1 Information architecture model	2.1
2.2 Corporate data dictionary and data syntax rules	2.2
2.3 Data classification scheme	2.3
2.4 Security levels	2.3
PO3 Determine technological direction.	
3.1 Technological infrastructure planning	3.1
3.2 Monitor future trends and regulations.	3.3
3.3 Technological infrastructure contingency	3.1
3.4 Hardware and software acquisition plans	3.1, AI3.1
3.5 Technology standards	3.4, 3.5
PO4 Define the IT organisation and relationships.	
4.1 IT planning or steering committee	4.3
4.2 Organisational placement of the IT function	4.4
4.3 Review of organisational achievements	4.5
4.4 Roles and responsibilities	4.6
4.5 Responsibility for quality assurance	4.7
4.6 Responsibility for logical and physical security	4.8
4.7 Ownership and custodianship	4.9
4.8 Data and system ownership	4.9
4.9 Supervision	4.10
4.10 Segregation of duties	4.11
4.11 IT staffing	4.12
4.12 Job or position descriptions for IT staff	4.6
4.13 Key IT personnel	4.13
4.14 Contracted staff policies and procedures	4.14
4.15 Relationships	4.15
PO5 Manage the IT investment.	
5.1 Annual IT operating budget	5.3
5.2 Cost and benefit monitoring	5.4
5.3 Cost and benefit justification	1.1, 5.3, 5.4, 5.5
PO6 Communicate management aims and direction.	
6.1 Positive information control environment	6.1
6.2 Management's responsibility for policies	6.3, 6.4, 6.5
6.3 Communication of organisation policies	6.3, 6.4, 6.5
6.4 Policy implementation resources	6.4
6.5 Maintenance of policies	6.3, 6.4, 6.5
6.6 Compliance with policies, procedures and standards	6.3, 6.4, 6.5
6.7 Quality commitment	6.3, 6.4, 6.5
6.8 Security and internal control framework policy	6.2
6.9 Intellectual property rights	6.3, 6.4, 6.5
6.10 Issue-specific policies	6.3, 6.4, 6.5
6.11 Communication of IT security awareness	6.3, 6.4, 6.5
PO7 Manage human resources.	
7.1 Personnel recruitment and promotion	7.1
7.2 Personnel qualifications	7.2
7.3 Roles and responsibilities	7.4
7.4 Personnel training	7.5
7.5 Cross-training or staff backup	7.6
7.6 Personnel clearance procedures	7.7
7.7 Employee job performance evaluation	7.8
7.8 Job change and termination	7.8
PO8 Ensure compliance with external requirements.	
8.1 External requirements review	ME3.1
8.2 Practices and procedures for complying with external requirements	ME3.2
8.3 Safety and ergonomic compliance	ME3.1
8.4 Privacy, intellectual property and data flow	ME3.1
8.5 Electronic commerce	ME3.1
8.6 Compliance with insurance contracts	ME3.1
PO9 Assess risks.	
9.1 Business risk assessment	9.1, 9.2, 9.4
9.2 Risk assessment approach	9.4
9.3 Risk identification	9.3
9.4 Risk measurement	9.1, 9.2, 9.3, 9.4
9.5 Risk action plan	9.5
9.6 Risk acceptance	9.5
9.7 Safeguard selection	9.5
9.8 Risk assessment committment	9.1
PO10 Manage projects.	
10.1 Project management framework	10.2
10.2 User department participation in project initiation	10.4
10.3 Project team membership and responsibilities	10.8
10.4 Project definition	10.5
10.5 Project approval	10.6
10.6 Project phase approval	10.6
10.7 Project master plan	10.7
10.8 System quality assurance plan	10.10
10.9 Planning of assurance methods	10.12
10.10 Formal project risk management	10.9
10.11 Test plan	AI7.2
10.12 Training plan	AI7.1
10.13 Post-implementation review plan	10.14 (part)
PO11 Manage quality.	
11.1 General quality plan	8.5
11.2 QA approach	8.1
11.3 QA planning	8.1
11.4 QA review of adherence to IT standards and procedures	8.1, 8.2
11.5 System development life cycle (SDLC) methodology	8.2, 8.3
11.6 SDLC methodology for major changes to existing technology	8.2, 8.3
11.7 Updating of the SDLC methodology	8.2, 8.3
11.8 Co-ordination and communication	8.2
11.9 Acquisition and maintenance framework for the technology infrastructure	8.2
11.10 Third-party implementor relationships	8.2, DS2.3
11.11 Programme documentation standards	AI4.2, AI4.3, AI4.4
11.12 Programme testing standards	AI7.2, AI7.4
11.13 System testing standards	AI7.2, AI7.4
11.14 Parallel/pilot testing	AI7.2, AI7.4
11.15 System testing documentation	AI7.2, AI7.4
11.16 QA evaluation of adherence to development standards	8.2
11.17 QA review of the achievement of IT objectives	8.2
11.18 Quality metrics	8.6
11.19 Reports of QA reviews	8.2

COBIT 3rd Edition	COBIT 4.1
AI1 Identify automated solutions.	
1.1 Definition of information requirements	1.1
1.2 Formulation of alternative courses of action	1.3, 5.1, PO1.4
1.3 Formulation of acquisition strategy	1.3, 5.1, PO1.4
1.4 Third-party service requirements	5.1, 5.3
1.5 Technological feasibility study	1.3
1.6 Economic feasibility study	1.3
1.7 Information architecture	1.3
1.8 Risk analysis report	1.2
1.9 Cost-effective security controls	1.1, 1.2
1.10 Audit trails design	1.1, 1.2
1.11 Ergonomics	1.1
1.12 Selection of system software	1.1, 1.3
1.13 Procurement control	5.1
1.14 Software product acquisition	5.1
1.15 Third-party software maintenance	5.4
1.16 Contract application programming	5.4
1.17 Acceptance of facilities	5.4
1.18 Acceptance of technology	3.1, 3.2, 3.3, 5.4
AI2 Acquire and maintain application software.	
2.1 Design methods	2.1
2.2 Major changes to existing systems	2.1, 2.2, 2.6
2.3 Design approval	2.1
2.4 File requirements definition and documentation	2.2
2.5 Programme specifications	2.2
2.6 Source data collection design	2.2
2.7 Input requirements definition and documentation	2.2
2.8 Definition of interfaces	2.2
2.9 User-machine interface	2.2
2.10 Processing requirements definition and documentation	2.2
2.11 Output requirements definition and documentation	2.2
2.12 Controllability	2.3, 2.4
2.13 Availability as a key design factor	2.2
2.14 IT integrity provisions in application programme software	2.3, DS11.5
2.15 Application software testing	2.8, 7.4
2.16 User reference and support materials	4.3. 4.4
2.17 Reassessment of system design	2.2
AI3 Acquire and maintain technology infrastructure.	
3.1 Assessment of new hardware and software	3.1, 3.2, 3.3
3.2 Preventive maintenance for hardware	DS13.5
3.3 System software security	3.1, 3.2, 3.3
3.4 System software installation	3.1, 3.2, 3.3
3.5 System software maintenance	3.3
3.6 System software change controls	6.1, 7.3
3.7 Use and monitoring of system utilities	3.2, 3.3, DS9.3
AI4 Develop and maintain procedures.	
4.1 Operational requirements and service levels	4.1
4.2 User procedures manual	4.2
4.3 Operations manual	4.4
4.4 Training materials	4.3, 4.4
AI5 Install and accredit systems.	
5.1 Training	7.1
5.2 Application software performance sizing	7.6, DS3.1
5.3 Implementation plan	7.2, 7.3
5.4 System conversion	7.5
5.5 Data conversion	7.5
5.6 Testing strategies and plans	7.2
5.7 Testing of changes	7.4, 7.6
5.8 Parallel/pilot testing criteria and performance	7.6
5.9 Final acceptance test	7.7
5.10 Security testing and accreditation	7.6
5.11 Operational test	7.6
5.12 Promotion to production	7.8
5.13 Evaluation of meeting user requirements	7.9
5.14 Management's post-implementation review	7.9
AI6 Manage changes.	
6.1 Change request initiation and control	61, 6.4
6.2 Impact assessment	6.2
6.3 Control of changes	7.9
6.4 Emergency changes	6.3
6.5 Documentation and procedures	6.5
6.6 Authorised maintenance	DS5.3
6.7 Software release policy	7.9
6.8 Distribution of software	7.9

COBIT 3rd Edition	COBIT 4.1
DS1 Define and manage service levels.	
1.1 SLA framework	1.1
1.2 Aspects of SLAs	1.3
1.3 Performance procedures	1.1
1.4 Monitoring and reporting	1.5
1.5 Review of SLAs and contracts	1.6
1.6 Chargeable items	1.3
1.7 Service improvement programme	1.6
DS2 Manage third-party services.	
2.1 Supplier interfaces	2.1
2.2 Owner relationships	2.2
2.3 Third-party contracts	AI5.2
2.4 Third-party qualifications	AI5.3
2.5 Outsourcing contracts	AI5.2
2.6 Continuity of services	2.3
2.7 Security relationships	2.3
2.8 Monitoring	2.4
DS3 Manage performance and capacity.	
3.1 Availability and performance requirements	3.1
3.2 Availability plan	3.4
3.3 Monitoring and reporting	3.5
3.4 Modelling tools	3.1
3.5 Proactive performance management	3.3
3.6 Workload forecasting	3.3
3.7 Capacity management of resources	3.2
3.8 Resources availability	3.4
3.9 Resources schedule	3.4
DS4 Ensure continuous service.	
4.1 IT continuity framework	4.1
4.2 IT continuity plan strategy and philosophy	4.1
4.3 IT continuity plan contents	4.2
4.4 Minimising IT continuity requirements	4.3
4.5 Maintaining the IT continuity plan	4.4
4.6 Testing the IT continuity plan	4.5
4.7 IT continuity plan training	4.6
4.8 IT continuity plan distribution	4.7
4.9 User department alternative processing backup procedures	4.8
4.10 Critical IT resources	4.3

COBIT 3rd Edition	COBIT 4.1
4.11 Backup site and hardware	4.8
4.12 Offsite backup storage	4.9
4.13 Wrap-up procedures	4.10
DS5 Ensure systems security.	
5.1 Manage security measures.	5.1
5.2 Identification, authentication and access	5.3
5.3 Security of online access to data	5.3
5.4 User account management	5.4
5.5 Management review of user accounts	5.4
5.6 User control of user accounts	5.4, 5.5
5.7 Security surveillance	5.5
5.8 Data classification	PO2.3
5.9 Central identification and access rights management	5.3
5.10 Violation and security activity reports	5.5
5.11 Incident handling	5.6
5.12 Reaccreditation	5.1
5.13 Counterparty trust	5.3, AC6
5.14 Transaction authorisation	5.3
5.15 Non-repudiation	5.11
5.16 Trusted path	5.11
5.17 Protection of security functions	5.7
5.18 Cryptographic key management	5.8
5.19 Malicious software prevention, detection and correction	5.9
5.20 Firewall architectures and connections with public networks	5.10
5.21 Protection of electronic value	13.4
DS6 Identify and allocate costs.	
6.1 Chargeable items	6.1
6.2 Costing procedures	6.3
6.3 User billing and chargeback procedures	6.2, 6.4
DS7 Educate and train users.	
7.1 Identification of training needs	7.1
7.2 Training organisation	7.2
7.3 Security principles and awareness training	PO7.4
DS8 Assist and advise customers.	
8.1 Help desk	8.1, 8.5
8.2 Registration of customer queries	8.2, 8.3, 8.4
8.3 Customer query escalation	8.3
8.4 Monitoring of clearance	10.3
8.5 Reporting and trend analysis	10.1
DS9 Manage the configuration.	
9.1 Configuration recording	9.1
9.2 Configuration baseline	9.1
9.3 Status accounting	9.3
9.4 Configuration control	9.3
9.5 Unauthorised software	9.3
9.6 Software storage	AI3.4
9.7 Configuration management procedures	9.2
9.8 Software accountability	9.1, 9.2
DS10 Manage problems and incidents.	
10.1 Problem management system	10.1, 10.2, 10.3, 10.4
10.2 Problem escalation	10.2
10.3 Problem tracking and audit trail	8.2, 10.2
10.4 Emergency and temporary access authorisations	5.4, 12.3, AI6.3
10.5 Emergency processing priorities	10.1, 8.3
DS11 Manage data.	
11.1 Data preparation procedures	AC1
11.2 Source document authorisation procedures	AC1
11.3 Source document data collection	AC1
11.4 Source document error handling	AC1
11.5 Source document retention	DS11.2
11.6 Data input authorisation procedures	AC2
11.7 Accuracy, completeness and authorisation checks	AC3
11.8 Data input error handling	AC2, AC4
11.9 Data processing integrity	AC4
11.10 Data processing validation and editing	AC4
11.11 Data processing error handling	AC4
11.12 Output handling and retention	AC5, 11.2
11.13 Output distribution	AC5, AC6
11.14 Output balancing and reconcilation	AC5
11.15 Output review and error handling	AC5
11.16 Security provision for output reports	11.6
11.17 Protection of sensitive information during transmission and transport	AC6, 11.6
11.18 Protection of disposed sensitive information	11.4, AC6
11.19 Storage management	11.2
11.20 Retention periods and storage terms	11.2
11.21 Media library management system	11.3
11.22 Media library management responsibilities	11.3
11.23 Backup and restoration	11.5
11.24 Backup jobs	11.4
11.25 Backup storage	4.9, 11.3
11.26 Archiving	11.2
11.27 Protection of sensitive messages	11.6
11.28 Authentication and integrity	AC6
11.29 Electronic transaction integrity	5.11
11.30 Continued integrity of stored data	11.2
DS12 Manage facilities.	
12.1 Physical security	12.1, 12.2
12.2 Low profile of the IT site	12.1, 12.2
12.3 Visitor escort	12.3
12.4 Personnel health and safety	12.1, 12.5, ME3.1
12.5 Protection against environmental factors	12.4, 12.9
12.6 Uninterruptible power supply	12.5
DS13 Manage operations.	
13.1 Processing operations procedures and instructions manual	13.1
13.2 Start-up process and other operations documentation	13.1
13.3 Job scheduling	13.2
13.4 Departures from standard job schedules	13.2
13.5 Processing continuity	13.1
13.6 Operation logs	13.1
13.7 Safeguard special forms and output devices	13.4
13.8 Remote operations	5.11

COBIT 3rd Edition	COBIT 4.1
M1 Monitor the processes.	
1.1 Collecting monitoring data	1.2
1.2 Assessing performance	1.4
1.3 Assessing customer satisfaction	1.2
1.4 Management reporting	1.5
M2 Assess internal control adequacy.	
2.1 Internal control monitoring	2.2
2.2 Timely operation of internal controls	2.1
2.3 Internal control level reporting	2.2, 2.3
2.4 Operational security and internal control assurance	2.4
M3 Obtain independent assurance.	
3.1 Independent security and internal control certification/accreditation of IT services	2.5, 4.7
3.2 Independent security and internal control certification/accreditation of third-party service providers	2.5, 4.7
3.3 Independent effectiveness evaluation of IT services	2.5, 4.7
3.4 Independent effectiveness evaluation of third-party service providers	2.5, 4.7
3.5 Independent assurance of compliance with laws, regulatory requirements and contractual commitments	2.5, 4.7
3.6 Independent assurance of compliance with laws, regulatory requirements and contractual commitments by third-party service providers	2.5, 2.6, 4.7
3.7 Competence of independent assurance function	2.5, 4.7
3.8 Proactive audit involvement	2.5, 4.7
M4 Provide for independent audit.	
4.1 Audit charter	2.5, 4.7
4.2 Independence	2.5, 4.7
4.3 Professional ethics and standards	2.5, 4.7
4.4 Competence	2.5, 4.7
4.5 Planning	2.5, 4.7
4.6 Performance of audit work	2.5, 4.7
4.7 Reporting	2.5, 4.7
4.8 Follow-up activities	2.5, 4.7

Cross-reference: COBIT 4.1 to COBIT 3rd Edition

COBIT 4.1	COBIT 3rd Edition
PO1 Define a strategic IT plan.	
1.1 IT value management	5.3
1.2 Business-IT alignment	New
1.3 Assessment of current capability and performance	1.7, 1.8
1.4 IT strategic plan	1.1, 1.2, 1.3, 1.4, 1.6, AI1.2, AI1.3
1.5 IT tactical plans	1.5
1.6 IT portfolio management	New
PO2 Define the information architecture.	
2.1 Enterprise information architecture model	2.1
2.2 Enterprise data dictionary and data syntax rules	2.2
2.3 Data classification scheme	2.3, 2.4, DS5.8
2.4 Integrity management	New
PO3 Determine technological direction.	
3.1 Technological direction planning	3.1, 3.3, 3.4
3.2 Technological infrastructure plan	New
3.3 Monitoring of future trends and regulations	3.2
3.4 Technology standards	3.5
3.5 IT architecture board	3.5
PO4 Define the IT processes, organisation and relationships.	
4.1 IT process framework	New
4.2 IT strategy committee	New
4.3 IT steering committee	4.1
4.4 Organisational placement of the IT function	4.2
4.5 IT organisational structure	4.3
4.6 Establishment of roles and responsibilities	4.4, 4.12
4.7 Responsibility for IT quality assurance	4.5
4.8 Responsibility for risk, security and compliance	4.6
4.9 Data and system ownership	4.7, 4.8
4.10 Supervision	4.9
4.11 Segregation of duties	4.10
4.12 IT staffing	4.11
4.13 Key IT personnel	4.13
4.14 Contracted staff policies and procedures	4.14
4.15 Relationships	4.15
PO5 Manage the IT investment.	
5.1 Financial management framework	New
5.2 Prioritisation within IT budget	New
5.3 IT budgeting	5.1, 5.3
5.4 Cost management	5.2, 5.3
5.5 Benefit management	5.3
PO6 Communicate management aims and direction.	
6.1 IT policy and control environment	6.1
6.2 Enterprise IT risk and control framework	6.8
6.3 IT policies management	6.2, 6.3, 6.5, 6.6, 6.7, 6.9, 6.10, 6.11
6.4 Policy, standards and procedures rollout	6.2, 6.3, 6.4, 6.5, 6.6, 6.7, 6.9, 6.10, 6.11
6.5 Communication of IT objectives and direction	6.2, 6.3, 6.5, 6.6, 6.7, 6.9, 6.10, 6.11
PO7 Manage IT human resources.	
7.1 Personnel recruitment and retention	7.1
7.2 Personnel competencies	7.2
7.3 Staffing of roles	New
7.4 Personnel training	7.3, DS7.3
7.5 Dependence upon individuals	7.4
7.6 Personnel clearance procedures	7.5
7.7 Employee job performance evaluation	7.6
7.8 Job change and termination	7.7, 7.8
PO8 Manage quality.	
8.1 Quality management system	11.2, 11.3, 11.4
8.2 IT standards and quality practices	11.5, 11.6, 11.7, 11.8, 11.9, 11.10, 11.16, 11.17, 11.19
8.3 Development and acquisition standards	11.5, 11.6, 11.7
8.4 Customer focus	New
8.5 Continuous improvement	New
8.6 Quality measurement, monitoring and review	11.18
PO9 Assess and manage IT risks.	
9.1 IT risk management framework	9.1, 9.4, 9.8
9.2 Establishment of risk context	9.1, 9.4
9.3 Event identification	9.3, 9.4
9.4 Risk assessment	9.1, 9.2, 9.4
9.5 Risk response	9.5, 9.6, 9.7
9.6 Maintenance and monitoring of a risk action plan	New
PO10 Manage projects.	
10.1 Programme management framework	New
10.2 Project management framework	10.1
10.3 Project management approach	New
10.4 Stakeholder commitment	10.2
10.5 Project scope statement	10.4
10.6 Project phase initiation	10.5, 10.6
10.7 Integrated project plan	10.7
10.8 Project resources	10.3
10.9 Project risk management	10.10
10.10 Project quality plan	10.8
10.11 Project change control	New
10.12 Project planning of assurance methods	10.9
10.13 Project performance measurement, reporting and monitoring	New
10.14 Project closure	10.13 (part)

COBIT 4.1	COBIT 3rd Edition
AI1 Identify automated solutions.	
1.1 Definition and maintenance of business functional and technical requirements	1.1, 1.9, 1.10, 1.11, 1.12
1.2 Risk analysis report	1.8, 1.9, 1.10
1.3 Feasibility study and formulation of alternative courses of action	1.3, 1.7, 1.12
1.4 Requirements and feasibility decision and approval	New
AI2 Acquire and maintain application software.	
2.1 High-level design	2.1, 2.2
2.2 Detailed design	2.2, 2.4, 2.5, 2.6, 2.7, 2.8, 2.9, 2.10, 2.11, 2.13, 2.17
2.3 Application control and auditability	2.12, 2.14
2.4 Application security and availability	2.12
2.5 Configuration and implementation of acquired application software	New
2.6 Major upgrades to existing systems	2.2
2.7 Development of application software	New
2.8 Software quality assurance	2.15
2.9 Applications requirements management	New

COBIT 4.1	COBIT 3rd Edition
2.10 Application software maintenance	New
AI3 Acquire and maintain technology infrastructure.	
3.1 Technological infrastructure acquisition plan	PO3.4, 1.18, 3.1, 3.3, 3.4
3.2 Infrastructure resource protection and availability	1.18, 3.1, 3.3, 3.4, 3.7
3.3 Infrastructure maintenance	1.18, 3.1, 3.3, 3.4, 3.5, 3.7
3.4 Feasibility test environment	New
AI4 Enable operation and use.	
4.1 Planning for operational solutions	4.1
4.2 Knowledge transfer to business management	PO11.11, 4.2
4.3 Knowledge transfer to end users	PO11.11, 2.16, 4.4
4.4 Knowledge transfer to operations and support staff	PO11.11, 2.16, 4.3, 4.4
AI5 Procure IT resources.	
5.1 Procurement control	1.2, 1.3, 1.4, 1.13, 1.14
5.2 Supplier contract management	DS2.3, DS2.5
5.3 Supplier selection	1.4, DS2.4
5.4 IT resources acquisition	1.15, 1.16, 1.17, 1.18
AI6 Manage changes.	
6.1 Change standards and procedures	3.6, 6.1

COBIT 4.1	COBIT 3rd Edition
6.2 Impact assessment, prioritisation and authorisation	6.2
6.3 Emergency changes	DS10.4, 6.4
6.4 Change status tracking and reporting	6.1
6.5 Change closure and documentation	6.5
AI7 Install and accredit solutions and changes.	
7.1 Training	PO10.11, PO10.12, 5.1
7.2 Test plan	PO10.11, PO11.12, PO11.13, PO11.14, PO11.15, 5.3, 5.6
7.3 Implementation plan	3.6, 5.3
7.4 Test environment	PO11.12, PO11.13, PO11.14, PO11.15, 2.15, 5.7
7.5 System and data conversion	5.4, 5.5
7.6 Testing of changes	5.2, 5.7, 5.8, 5.10, 5.11
7.7 Final acceptance test	5.9
7.8 Promotion to production	5.12
7.9 Post-implementation review	5.13, 5.14

COBIT 4.1	COBIT 3rd Edition
DS1 Define and manage service levels.	
1.1 Service level management framework	1.1, 1.3
1.2 Definition of services	New
1.3 SLAs	1.2, 1.6
1.4 OLAs	New
1.5 Monitoring and reporting of service level achievements	1.4
1.6 Review of SLAs and contracts	1.5, 1.7
DS2 Manage third-party services.	
2.1 Identification of all supplier relationships	2.1
2.2 Supplier relationship management	2.2
2.3 Supplier risk management	PO11.10, 2.6, 2.7
2.4 Supplier performance monitoring	2.8

COBIT 4.1	COBIT 3rd Edition
DS3 Manage performance and capacity.	
3.1 Performance and capacity planning	AI5.2, 3.1, 3.4
3.2 Current performance and capacity	3.7
3.3 Future performance and capacity	3.5, 3.6
3.4 IT resources availability	3.2, 3.8, 3.9
3.5 Monitoring and reporting	3.3
DS4 Ensure continuous service.	
4.1 IT continuity framework	4.1, 4.2
4.2 IT continuity plans	4.3
4.3 Critical IT resources	4.4, 4.10
4.4 Maintenance of the IT continuity plan	4.5
4.5 Testing of the IT continuity plan	4.6
4.6 IT continuity plan training	4.7
4.7 Distribution of the IT continuity plan	4.8

COBIT 4.1	COBIT 3rd Edition
4.8 IT services recovery and resumption	4.9, 4.11
4.9 Offsite backup storage	4.12, 11.25
4.10 Post-resumption review	4.13
DS5 Ensure systems security.	
5.1 Management of IT security	5.1, 5.12
5.2 IT security plan	New
5.3 Identity management	5.2, 5.3, 5.9, 5.14, AI6.6
5.4 User account management	5.4, 5.5, 5.6, 5.13, 10.4
5.5 Security testing, surveillance and monitoring	5.6, 5.7, 5.10
5.6 Security incident definition	5.11
5.7 Protection of security technology	5.17
5.8 Cryptographic key management	5.18

COBIT 4.1	COBIT 3rd Edition
5.9 Malicious software prevention, detection and correction	5.19
5.10 Network security	5.20
5.11 Exchange of sensitive data	5.15, 5.16 11.29, 13.8
DS6 Identify and allocate costs.	
6.1 Definition of services	6.1
6.2 IT accounting	6.3
6.3 Cost modelling and charging	6.2
6.4 Cost model maintenance	6.3
DS7 Educate and train users.	
7.1 Identification of education and training needs	7.1
7.2 Delivery of training and education	7.2
7.3 Evaluation of training received	New
DS8 Manage service desk and incidents.	
8.1 Service desk	8.1
8.2 Registration of customer queries	8.2, 10.3
8.3 Incident escalation	8.2, 8.3, 10.5
8.4 Incident closure	8.2
8.5 Reporting and trend analysis	8.1
DS9 Manage the configuration.	
9.1 Configuration repository and baseline	9.1, 9.2, 9.8
9.2 Identification and maintenance of configuration items	9.7, 9.8
9.3 Configuration integrity review	9.3, 9.4, 9.5
DS10 Manage problems.	
10.1 Identification and classification of problems	8.5, 10.1, 10.5
10.2 Problem tracking and resolution	New
10.3 Problem closure	8.4, 10.1
10.4 Integration of configuration, incident and problem management	New, 10.1
DS11 Manage data.	
11.1 Business requirements for data management	New
11.2 Storage and retention arrangements	11.12, 11.19, 11.20, 11.26, 11.30
11.3 Media library management system	11.21, 11.22, 11.25
11.4 Disposal	11.18, 11.24
11.5 Backup and restoration	AI2.14, 11.23
11.6 Security requirements for data management	11.16, 11.17, 11.27
DS12 Manage the physical environment.	
12.1 Site selection and layout	12.1, 12.2, 12.4
12.2 Physical security measures	12.1, 12.2
12.3 Physical access	10.4, 12.3
12.4 Protection against environmental factors	12.5
12.5 Physical facilities management	12.4, 12.6, 12.9
DS13 Manage operations.	
13.1 Operations procedures and instructions	13.1, 13.2, 13.5, 13.6
13.2 Job scheduling	13.3, 13.4
13.3 IT infrastructure monitoring	New
13.4 Sensitive documents and output devices	5.21, 13.7
13.5 Preventive maintenance for hardware	AI3.2

COBIT 4.1	COBIT 3rd Edition
ME1 Monitor and evaluate IT performance.	
1.1 Monitoring approach	1.0*
1.2 Definition and collection of monitoring data	1.1, 1.3
1.3 Monitoring method	New
1.4 Performance assessment	1.2
1.5 Board and executive reporting	1.4
1.6 Remedial actions	New
ME2 Monitor and evaluate internal control.	
2.1 Monitoring of internal control framework	2.0*, 2.2
2.2 Supervisory review	2.1, 2.3
2.3 Control exceptions	New
2.4 Control self-assessment	2.4
2.5 Assurance of internal control	New
2.6 Internal control at third parties	3.6
2.7 Remedial actions	New
ME3 Ensure compliance with external requirements.	
3.1 Identification of external legal, regulatory and contractual compliance requirements	PO8.1, PO8.3, PO8.4, PO8.5, PO8.6, DS12.4
3.2 Optimisation of response to external requirements	PO8.2
3.3 Evaluation of compliance with external requirements	New
3.4 Positive assurance of compliance	New
3.5 Integrated reporting	New
ME4 Provide IT governance.	
4.1 Establishment of an IT governance framework	New
4.2 Strategic alignment	New
4.3 Value delivery	New
4.4 Resource management	New
4.5 Risk management	New
4.6 Performance measurement	New
4.7 Independent assurance	New

* ME1.0 and ME2.0 introduced in *Control Practices* published by ITGI in 2004.

Appendix VI

Approach to Research and Development

Appendix VI
Approach

Appendix VI—Approach to Research and Development

Development of the CobiT framework content is supervised by the CobiT Steering Committee, formed by international representatives from industry, academia, government, and the IT governance, assurance, control and security profession. International working groups have been established for the purpose of quality assurance and expert review of the project's interim research and development deliverables. Overall project guidance is provided by ITGI.

PREVIOUS CobiT EDITIONS

Starting with the CobiT framework defined in the first edition, the application of international standards, guidelines and research into good practices led to the development of the control objectives. Audit guidelines were next developed to assess whether these control objectives are appropriately implemented. Research for the first and second editions included the collection and analysis of identified international sources and was carried out by teams in Europe (Free University of Amsterdam), the US (California Polytechnic University) and Australia (University of New South Wales). The researchers were charged with the compilation, review, assessment and appropriate incorporation of international technical standards, codes of conduct, quality standards, professional standards in auditing, and industry practices and requirements, as they relate to the framework and to individual control objectives. After collection and analysis, the researchers were challenged to examine each domain and process in depth, and suggest new or modified control objectives applicable to that particular IT process. Consolidation of the results was performed by the CobiT Steering Committee.

The CobiT 3rd Edition project consisted of developing the management guidelines and updating CobiT 2nd Edition based on new and revised international references. Furthermore, the CobiT framework was revised and enhanced to support increased management control, introduce performance management and further develop IT governance. To provide management with an application of the framework, so it can assess and make choices for control implementation and improvements over its information and related technology, as well as measure performance, the management guidelines include maturity models, critical success factors, KGIs and KPIs related to the control objectives.

The management guidelines were developed by using a worldwide panel of 40 experts from academia, government, and the IT governance, assurance, control and security profession. These experts participated in a residential workshop guided by professional facilitators and using development guidelines defined by the CobiT Steering Committee. The workshop was strongly supported by the Gartner Group and PricewaterhouseCoopers, who not only provided thought leadership but also sent several of their experts on control, performance management and information security. The results of the workshop were draft maturity models, CSFs, KGIs and KPIs for each of CobiT's 34 process descriptions. Quality assurance of the initial deliverables was conducted by the CobiT Steering Committee, and the results were posted for exposure on the ISACA web site. The management guidelines document offered a new management-oriented set of tools, while providing integration and consistency with the CobiT framework.

The update to the control objectives in CobiT 3rd Edition, based on new and revised international references, was conducted by members of ISACA chapters, under the guidance of CobiT Steering Committee members. The intention was not to perform a global analysis of all material or a redevelopment of the control objectives, but to provide an incremental update process. The results of the development of the management guidelines were then used to revise the CobiT framework, especially the considerations, goals and enabler statements of the process descriptions. CobiT 3rd Edition was published in July 2000.

THE LATEST UPDATE PROJECT ACTIVITY

In its effort to continuously evolve the CobiT body of knowledge, the CobiT Steering Committee has initiated over the last two years research into several detailed aspects of CobiT. These focused research projects addressed components of the control objectives and the management guidelines. Some specific areas that were addressed follow.

Control Objectives Research

- CobiT—IT governance bottom-up alignment
- CobiT—IT governance top-down alignment
- CobiT and other detailed standards—Detailed mapping between CobiT and ITIL, CMM, COSO, PMBOK, ISF's *Standard of Good Practice for Information Security* and ISO 27000 to enable harmonisation with those standards in language, definitions and concepts

Management Guidelines Research

- KGI-KPI causal relationships analysis
- Review of the quality of the KGIs/KPIs/CSFs—Based on the KPI/KGI causal relationship analysis, splitting CSFs into 'what you need from others' and 'what you need to do yourself'
- Detailed analysis of metrics concepts—Detailed development with metrics experts to enhance the metrics concepts, building up a cascade of 'process-IT-business' metrics and defining quality criteria for metrics
- Linking of business goals, IT goals and IT processes—Detailed research in eight different industries resulting in a more detailed insight into how COBIT processes support the achievement of specific IT goals and, by extension, business goals; results then generalised
- Review of maturity model contents—Ensured consistency and quality of maturity levels between and within processes, including better definitions of maturity model attributes

All of these projects were initiated and overseen by the COBIT Steering Committee, while day-to-day management and follow-up were executed by a smaller COBIT core team. The execution of most of the aforementioned research projects was based heavily on the expertise and volunteer team of ISACA members, COBIT users, expert advisors and academics. Local development groups were set up in Brussels (Belgium), London (England), Chicago (Illinois, USA), Canberra (Australian Capital Territory), Cape Town (South Africa), Washington (DC, USA) and Copenhagen (Denmark), in which five to 10 COBIT users gathered on average two to three times per year to work on specific research or review tasks assigned by the COBIT core team. In addition, some specific research projects were assigned to business schools such as the University of Antwerp Management School (UAMS) and the University of Hawaii.

The results of these research efforts, together with feedback provided by COBIT users over the years and issues noted from the development of new products such as the control practices, have been fed into the main COBIT project to update and improve the COBIT control objectives, management guidelines and framework. Two major development labs, each involving more than 40 IT governance, management and control experts (managers, consultants, academics and auditors) from around the world, were held to review and thoroughly update the control objectives and management guidelines content. Further smaller groups worked on refining or finalising the significant output produced by these major events.

The final draft was subject to a full exposure review process with approximately 100 participants. The extensive comments received were analysed in a final review workshop by the COBIT Steering Committee.

The results of these workshops have been processed by the COBIT Steering Committee, the COBIT core team and ITGI to create the new COBIT material available in this volume. The existence of COBIT Online means that the technology now exists to keep the core COBIT content up to date more easily, and this resource will be used as the master repository of COBIT content. It will be maintained by feedback from the user base as well as periodic reviews of specific content areas. Periodic publications (paper and electronic) will be produced to support offline reference to COBIT content.

Appendix VII

Glossary

APPENDIX VII—GLOSSARY

Access control —The process that limits and controls access to resources of a computer system; a logical or physical control designed to protect against unauthorised entry or use

Accountable—In a RACI chart, refers to the person or group who has the authority to approve or accept the execution of an activity

Activity—The main actions taken to operate the COBIT process

Application program—A program that processes business data through activities such as data entry, update or query. It contrasts with systems programs, such as an operating system or network control program, and with utility programs, such as *copy* or *sort*.

Audit charter—A document approved by the board, which defines the purpose, authority and responsibility of the internal audit activity

Authentication—The act of verifying the identity of a system entity (e.g., user, system, network node) and the entity's eligibility to access computerised information. Designed to protect against fraudulent logon activity, authentication can also refer to the verification of the correctness of a piece of data.

Automated application control—A set of controls embedded within automated solutions (applications)

Balanced scorecard—A coherent set of performance measures organised into four categories. It includes traditional financial measures, but adds customer, internal business process, and learning and growth perspectives. It was developed by Robert S. Kaplan and David P. Norton in 1992.

Benchmarking—A systematic approach to comparing an organisation's performance against peers and competitors in an effort to learn the best ways of conducting business (e.g., benchmarking of quality, logistical efficiency and various other metrics)

Best practice—A proven activity or process that has been successfully used by multiple organisations

Business process—See Process.

Capability—Having the needed attributes to perform or accomplish

Capability Maturity Model (CMM)—The CMM for Software, from the Software Engineering Institute (SEI). A model used by many organisations to identify good practices useful in helping them assess and increase the maturity of their software development processes.

CEO—Chief executive officer; the highest-ranking individual in an organisation

CFO—Chief financial officer; the individual primarily responsible for managing the financial risks of an organisation

CIO—Chief information officer; the individual responsible for the IT group within an organisation. In some cases, the CIO role has been expanded to become the chief knowledge officer (CKO), who deals in knowledge, not just information. Also see CTO.

CTO—Chief technology officer; focuses on technical issues in an organisation. The title CTO is often viewed as synonymous with CIO.

Configuration item (CI)—Component of an infrastructure—or an item, such as a request for change, associated with an infrastructure—which is (or is to be) under the control of configuration management. CIs may vary widely in complexity, size and type, from an entire system (including all hardware, software and documentation) to a single module or a minor hardware component.

Configuration management—The control of changes to a set of configuration items over a system life cyle

Consulted—In a RACI chart, refers to those people whose opinions are sought on an activity (two-way communication)

Continuity—Preventing, mitigating and recovering from disruption. The terms 'business resumption planning', 'disaster recovery planning' and 'contingency planning' also may be used in this context; they all concentrate on the recovery aspects of continuity.

Control framework—A set of fundamental controls that facilitates the discharge of business process owner responsibilities to prevent financial or information loss in an organisation

Control objective—A statement of the desired result or purpose to be achieved by implementing control procedures in a particular process

Control practice—Key control mechanism that supports the achievement of control objectives through responsible use of resources, appropriate management of risk and alignment of IT with business

COSO—Committee of Sponsoring Organisations of the Treadway Commission. Its 1992 report *Internal Control—Integrated Framework* is an internationally accepted standard for corporate governance. See *www.coso.org*.

CSF—Critical success factor; the most important issues or actions for management to achieve control over and within its IT processes

Dashboard—A tool for setting expectations for an organisation at each level of responsibility and continuous monitoring of the performance against set targets

Data classification scheme—An enterprisewide scheme for classifying data by factors such as criticality, sensitivity and ownership

Data dictionary—A database that contains the name, type, range of values, source and authorisation for access for each data element in a database. It also indicates which application programs use that data so that when a data structure is contemplated, a list of the affected programs can be generated. The data dictionary may be a stand-alone information system used for management or documentation purposes, or it may control the operation of a database.

Data owners—Individuals, normally managers or directors, who have responsibility for the integrity, accurate reporting and use of computerised data

Detective control—A control that is used to identify events (undesirable or desired), errors and other occurrences that an enterprise has determined to have a material effect on a process or end product

Domain—In COBIT, the grouping of control objectives into logical stages in the IT life cycle of investments involving IT (Plan and Organise, Acquire and Implement, Deliver and Support, and Monitor and Evaluate)

Enterprise—A group of individuals working together for a common purpose, typically within the context of an organisational form such as a corporation, public agency, charity or trust

Enterprise architecture—Description of the fundamental underlying design of the components of the business system, or of one element of the business system (e.g., technology), the relationships amongst them and the manner in which they support the organisation's objectives

Enterprise architecture for IT—Description of the fundamental underlying design of the IT components of the business, the relationships amongst them and the manner in which they support the organisation's objectives

Enterprise governance—A set of responsibilities and practices exercised by the board and executive management with the goal of providing strategic direction, ensuring that objectives are achieved, ascertaining that risks are managed appropriately and verifying that the enterprise's resources are used responsibly

Framework—See Control framework.

General computer controls—Controls, other than application controls, which relate to the environment within which computer-based application systems are developed, maintained and operated, and which are therefore applicable to all applications. The objectives of general controls are to ensure the proper development and implementation of applications, the integrity of program and data files and of computer operations. Like application controls, general controls may be either manual or programmed. Examples of general controls include the development and implementation of an IS strategy and an IS security policy, the organisation of IS staff to separate conflicting duties, and planning for disaster prevention and recovery.

Guideline—A description of a particular way of accomplishing something that is less prescriptive than a procedure

Information architecture—One component of IT architecture (together with applications and technology). See IT architecture.

Informed—In a RACI chart, refers to those people who are kept up to date on the progress of an activity (one-way communication)

Internal control —The policies, plans and procedures, and organisational structures designed to provide reasonable assurance that business objectives will be achieved and undesired events will be prevented or detected and corrected

ISO 17799—An international standard that defines information confidentiality, integrity and availability controls

ISO 277001—*Information Security Management—Specification with Guidance for Use*; the replacement for BS7799-2. It is intended to provide the foundation for third-party audit and is harmonised with other management standards, such as ISO/IEC 9001 and 14001.

ISO 9001:2000—Code of practice for quality management from the International Organisation for Standardisation (ISO). ISO 9001:2000, which specifies requirements for a quality management system for any organisation that needs to demonstrate its ability to consistently provide product or service that meets particular quality targets.

IT—Information technology; the hardware, software, communications and other facilities used to input, store, process, transmit and output data in whatever form

IT architecture—Description of the fundamental underlying design of the IT components of the business, the relationships amongst them and the manner in which they support the organisation's objectives

ITIL—The UK Office of Government Commerce (OGC) IT Infrastructure Library; a set of guides on the management and provision of operational IT services

IT incident—Any event that is not part of the ordinary operation of a service and that causes, or may cause, an interruption to, or a reduction in, the quality of that service (aligned to ITIL)

IT investment dashboard—A tool for setting expectations for an organisation at each level and continuous monitoring of the performance against set targets for expenditures on and returns from IT-enabled investment projects in terms of business values

IT strategic plan—A long-term plan, i.e., three- to five-year horizon, in which business and IT management co-operatively describe how IT resources will contribute to the enterprise's strategic objectives (goals)

IT strategy committee—Committee at the level of the board of directors to ensure that the board is involved in major IT matters/decisions. The committee is primarily accountable for managing the portfolios of IT-enabled investments, IT services and other IT resources. The committee is the owner of the portfolio.

IT tactical plan—A medium-term plan, i.e., six- to 18-month horizon, that translates the IT strategic plan direction into required initiatives, resource requirements, and ways in which resources and benefits will be monitored and managed

IT user—A person who uses IT to support or achieve a business objective

Key management practices—Those management practices required to successfully execute business processes

KGI—Key goal indicator; measures that tell management, after the fact, whether an IT process has achieved its business requirements, usually expressed in terms of information criteria

KPI—Key performance indicator; measures that determine how well the process is performing in enabling the goal to be reached. They are lead indicators of whether a goal will likely be reached, and are good indicators of capabilities, practices and skills. They measure the activity goals, which are the actions the process owner must take to achieve effective process performance.

Maturity—In business, indicates the degree of reliability or dependency the business can place on a process achieving the desired goals or objectives

Measure—A standard used to evaluate and communicate performance against expected results. Measures are normally quantitative in nature capturing numbers, dollars, percentages, etc., but can also address qualitative information such as customer satisfaction. Reporting and monitoring measures help an organisation gauge progress toward effective implementation of strategy.

Metrics—Specific descriptions of how a quantitative and periodic assessment of performance is to be measured. A complete metric defines the unit used, frequency, ideal target value, the procedure to carry out the measurement and the procedure for the interpretation of the assessment.

OLA—Operational level agreement; an internal agreement covering the delivery of services that support the IT organisation in its delivery of services

Organisation—The manner in which an enterprise is structured; can also mean the entity

Outcome measures—Measures that represent the consequences of actions previously taken and are often referred to as lag indicators. They frequently focus on results at the end of a time period and characterise historical performance. They are also referred to as key goal indicators (KGIs) and are used to indicate whether goals have been met. These can be measured only after the fact and, therefore, are called 'lag indicators'.

Performance—In IT, the actual implementation or achievement of a process

Performance drivers—Measures that are considered the 'drivers' of lag indicators. They can be measured before the outcome is clear and, therefore, are called 'lead indicators'. There is an assumed relationship between the two that suggests that improved performance in a leading indicator will drive better performance in the lagging indicator. They are also referred to as key performance indicators (KPIs) and are used to indicate whether goals are likely to be met.

Performance management—In IT, the ability to manage any type of measurement, including employee, team, process, operational or financial measurements. The term connotes closed-loop control and regular monitoring of the measurement.

PMBOK—Project Management Body of Knowledge; a project management standard developed by the Project Management Institute (PMI)

PMO—Project management officer; the individual function responsible for the implementation of a specified initiative for supporting the project management role and advancing the discipline of project management

Policy—Generally, a document that records a high-level principle or course of action that has been decided upon. A policy's intended purpose is to influence and guide both present and future decision making to be in line with the philosophy, objectives and strategic plans established by the enterprise's management teams. In addition to policy content, policies need to describe the consequences of failing to comply with the policy, the means for handling exceptions, and the manner in which compliance with the policy will be checked and measured.

Portfolio—A grouping of programmes, projects, services or assets selected, managed and monitored to optimise business return

Preventive control—An internal control that is used to prevent undesirable events, errors and other occurrences that an organisation has determined could have a negative material effect on a process or end product

PRINCE2—Projects in a Controlled Environment, developed by the OGC; a project management method that covers the management, control and organisation of a project

Problem—In IT, the unknown underlying cause of one or more incidents

Procedure—A document containing steps that specify how to achieve an activity. Procedures are defined as part of processes.

Process—Generally, a collection of procedures influenced by the organisation's policies and procedures that takes inputs from a number of sources, including other processes, manipulates the inputs, and produces outputs, including other processes. Processes have clear business reasons for existing, accountable owners, clear roles and responsibilities around the execution of the process, and the means to measure performance.

Programme—A structured grouping of interdependent projects that includes the full scope of business, process, people, technology and organisational activities that are required (both necessary and sufficient) to achieve a clearly specified business outcome

Project—A structured set of activities concerned with delivering to the enterprise a defined capability (that is necessary but not sufficient to achieve a required business outcome) based on an agreed-upon schedule and budget

QMS—Quality management system; a system that outlines the policies and procedures necessary to improve and control the various processes that will ultimately lead to improved organisation performance

RACI chart—Illustrates who is responsible, accountable, consulted and informed within an organisational framework

Resilience—In business, the ability of a system or network to recover automatically from any disruption, usually with minimal recognisable effect

Responsible—In a RACI chart, refers to the person who must ensure that activities are completed successfully

Risk—In business, the potential that a given threat will exploit vulnerabilities of an asset or group of assets to cause loss and/or damage to the assets; usually measured by a combination of impact and probability of occurrence

Root cause analysis—Process of diagnosis to establish origins of events, which can be used for learning from consequences, typically of errors and problems

SDLC—System development life cycle; the phases deployed in the development or acquisition of a software system. Typical phases include the feasibility study, requirements study, requirements definition, detailed design, programming, testing, installation and post-implementation review, but not the service delivery or benefits realisation activities.

Segregation/separation of duties—A basic internal control that prevents or detects errors and irregularities by assigning to separate individuals responsibility for initiating and recording transactions and custody of assets to separate individuals. Commonly used in large IT organisations so that no single person is in a position to introduce fraudulent or malicious code without detection.

Service desk—A point of contact within the IT organisation for users of IT services

Service provider—External entity that provides services to the organisation

SLA—Service level agreement; an agreement, preferably documented, between a service provider and the customer(s)/user(s) that defines minimum performance targets for a service and how they will be measured

Standard—A mandatory requirement. Examples include ISO/IEC 20000 (an international standard), an internal security standard for UNIX configuration or a government standard for how financial records should be maintained. The term 'standard' is also used to refer to a code of practice or specifications published by a standards organisation, such as ISO or BSI.

TCO—Total cost of ownership; in IT includes:
- Original cost of the computer and software
- Hardware and software upgrades
- Maintenance
- Technical support
- Training
- Certain activities performed by users

Technology infrastructure plan—A plan for the technology, human resources and facilities that enables the current and future processing and use of applications

Page intentionally left blank

Appendix VIII

CobiT and Related Products

Appendix VIII—CobiT and Related Products

The CobiT framework, in versions 4.0 and higher, includes all of the following:
- Framework—Explains how CobiT organises IT governance management and control objectives and good practices by IT domains and processes, and links them to business requirements
- Process descriptions—Include 34 IT processes covering the IT responsibility areas from beginning to end
- Control objectives—Provide generic best practice management objectives for IT processes
- Management guidelines—Offer tools to help assign responsibility, measure performance, and benchmark and address gaps in capability
- Maturity models—Provide profiles of IT processes describing possible current and future states

In the years since its inception, CobiT's core content has continued to evolve, and the number of CobiT-based derivative works has increased. Following are the publications currently derived from CobiT:
- *Board Briefing on IT Governance, 2nd Edition*—Designed to help executives understand why IT governance is important, what its issues are and what their responsibility is for managing it
- CobiT Online—Allows users to customise a version of CobiT for their own enterprise, then store and manipulate that version as desired. It offers online, real-time surveys, frequently asked questions, benchmarking and a discussion facility for sharing experiences and questions.
- *CobiT Control Practices: Guidance to Achieve Control Objectives for Successful IT Governance, 2nd Edition*—Provides guidance on the risks to be avoided and value to be gained from implementing a control objective, and instruction on how to implement the objective. Control practices are strongly recommended for use with the *IT Governance Implementation Guide: Using CobiT and Val IT, 2nd Edition.*
- *IT Assurance Guide: Using CobiT*—Provides guidance on how CobiT can be used to support a variety of assurance activities and offers suggested testing steps for all the CobiT IT processes and control objectives. It replaces the information in *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*—Provides a baseline of control for the smaller organisation and a possible first step for the larger enterprise
- CobiT *Security Baseline*—Focuses on essential steps for implementing information security within the enterprise. The second edition is in development at the time of this writing.
- CobiT Mappings—Currently posted at *www.isaca.org/downloads*:
  - *Aligning CobiT, ITIL and ISO 17799 for Business Benefit*
  - *CobiT Mapping: Overview of International IT Guidance, 2nd Edition*
  - *CobiT Mapping: Mapping of ISO/IEC 17799:2000 With CobiT, 2nd Edition*
  - *CobiT Mapping: Mapping of PMBOK With CobiT 4.0*
  - *CobiT Mapping: Mapping of SEI's CMM for Software With CobiT 4.0*
  - *CobiT Mapping: Mapping of ITIL With CobiT 4.0*
  - *CobiT Mapping: Mapping of PRINCE2 With CobiT 4.0*
- *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*, which explains how an enterprise can extract optimal value from IT-enabled investments and is based on the CobiT framework. It is organised into:
  - Three processes—Value Governance, Portfolio Management and Investment Management
  - IT key management practices—Essential management practices that positively influence the achievement of the desired result or purpose of a particular activity. They support the Val IT processes and play roughly the same role as do CobiT's control objectives.
- *Enterprise Value: Governance of IT Investments—The Business Case*, which focuses on one key element of the investment management process
- *Enterprise Value: Governance of IT Investments—The ING Case Study*, which describes how a global financial services company manages a portfolio of IT investments in the context of the Val IT framework

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

Page intentionally left blank

IT GOVERNANCE INSTITUTE®

LEADING THE IT GOVERNANCE COMMUNITY

3701 ALGONQUIN ROAD, SUITE 1010
ROLLING MEADOWS, IL 60008 USA
PHONE: +1.847.590.7491
FAX: +1.847.253.1443
E-MAIL: *info@itgi.org*
WEB SITE: *www.itgi.org*