GOVERNANCE INSTITUTE®

LEADING THE IT GOVERNANCE COMMUNITY

IT ASSURANCE GUIDE

USING COBIT®

Need for IT Governance and Assurance

The COBIT® Framework

IT Assurance Approaches

How COBIT Supports IT Assurance Activities

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 *IT Assurance Guide: Using COBIT®* (the 'Work'), primarily as an educational resource for assurance 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.

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 1-933284-74-9
IT Assurance Guide: Using COBIT®
Printed in the United States of America

ACKNOWLEDGEMENTS

IT Governance Institute wishes to recognise:

Project Managers and Thought Leaders
Roger S. Debreceny, Ph.D., FCPA, University of Hawaii, USA
Erik Guldentops, CISA, CISM, University of Antwerp Management School, Belgium

Workshop Participants and Expert Reviewers
Mark Adler, CISA, CISM, CIA, CISSP, Allstate Insurance 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 Caniglia, CISA, CISM, USA
Luis A. Capua, CISM, Sindicatura General de la Nación, Argentina
Boyd Carter, PMP, Elegantsolutions.ca, Canada
Sean V. Casey, CISA, CPA, Ernst & Young LLP, USA
Sushil Chatterji, Edutech, Singapore
Ed Chavennes, CISA, 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
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, South Africa
Troy DuMoulin, Pink Elephant, Canada
Bill A. Durrand, CISA, CISM, CA, Ernst & Young LLP, Canada
Justus Ekeigwe, CISA, MBCS, Deloitte & Touche LLP, USA
Rafael Fabius, CISA, República AFAP SA, Uruguay
Urs Fischer, CISA, CIA, CPA (Swiss), Swiss Life, Switzerland
Christopher Fox, ACA, 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
Benjamin K. Hsaio, CISA, Federal Deposit Insurance Corp., USA
Tom Hughes, Acumen Alliance, Australia
Monica Jain, CSQA, Covansys Corp., US
Avinash W. Kadam, CISA, CISM, CBCP, CISSP, MIEL e-Security Pvt. Ltd., India
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

Lynn Lawton, CISA, BA, FCA, FIIA, PII, KPMG LLP, UK
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
Bjarne Lonberg, CISSP, A.P. Moller-Maersk A/S, Denmark
Donald Lorete, CPA, Deloitte & Touche LLP, USA
Addie C.P. Lui, MCSA, MCSE, First Hawaiian Bank, 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
Orillo Narduzzo, CISA, CISM, Banca Popolare di Vicenza, Italy
Sang Nguyen, CISA, CISSP, MCSE, Nova Southeastern University, USA
Anthony Noble, CISA, CCP, Viacom Inc., USA
Ed O'Donnell, Ph.D., CPA, University of Kansas, USA
Sue Owen, Department of Veterans Affairs, Australia
Robert G. Parker, CISA, CMC, FCA, Robert G. Parker Consulting, Canada
Bart Peeters, PricewaterhouseCoopers LLP, Belgium
Thomas Phelps IV, CISA, PricewaterhouseCoopers LLP, USA
Vitor Prisca, CISM, Novabase, Portugal
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
Gustavo A. Solis, CISA, CISM, Grupo Cynthus, Mexico
Roger Southgate, CISA, CISM, FCCA, CubeIT Management Ltd., UK
Paula Spinner, CSC, USA
Mark Stanley, CISA, Toyota Financial Services, USA
Dirk 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
Ingvar Van Droogenbroeck, PricewaterhouseCoopers, Belgium
Wim Van Grembergen, Ph.D., University of Antwerp Management School, Belgium
Johan Van Grieken, CISA, Deloitte, Belgium
Greet Volders, Voquals NV, Belgium
Robert M. Walters, CISA, CPA, CGA, Office of the Comptroller General, Canada
Tom Wong, CISA, CIA, CMA, Ernst & Young LLP, Canada
Amanda Xu, CISA, PMP, KPMG LLP, USA

The following professors and students for their work on the CobiT 4.1 control practices and assurance test steps
Scott L. Summers, Ph.D., Brigham Young University, USA
Keith Ballante, Brigham Young University, USA
David Butler, Brigham Young University, USA
Phil Harrison, Brigham Young University, USA
William Lancaster, Brigham Young University, USA
Chase Manderino, Brigham Young University, USA
Paul Schneider, Brigham Young University, USA
Jacob Sperry, Brigham Young University, USA
Brian Updike, Brigham Young University, USA

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 and IGM Financial, Canada

Assurance Committee
Lynn C. Lawton, CISA, BA, FCA, FIIA, PII, KPMG LLP, UK
Pippa G. Andrews, CISA, ACA, CIA, Amcor, Australia
John Warner Beveridge, CISA, CISM, CFE, CGFM, Office of the Massachusetts State Auditor, USA
Daniel Patrick Casciano, CISA, Ernst & Young LLP, USA
Gregory T. Grocholski, CISA, The Dow Chemical Company, USA
Avinash W. Kadam, CISA, CISM, CBCP, CISSP, MIEL e-Security Pvt. Ltd., India
Anthony P. Noble, CISA, CCP, Viacom Inc., USA
Gustavo A. Solis, Grupo Cynthus S.A. de C.V., Mexico
Paul A. Zonneveld, CISA, CA, Deloitte & Touche, Canada
Corresponding Member Robert G. Parker, CISA, CA, CMC, FCA, Canada

COBIT Steering Committee
Roger S. 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 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 LLP, Austria
Debbie Lew, CISA, Ernst & Young LLP, USA
Max Shanahan, FCPA, CISA, Max Shanahan & Associates, Australia
Dirk Steuperaert, CISA, PricewaterhouseCoopers, Belgium
Robert E. Stroud, CA Inc., USA

ITGI Advisory Panel
Ronald Saull, CSP, Great-West Life 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 of 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 (ISSA)
Institut de la Gouvernance des Systèmes d'Information
Institute of Management Accountants
ISACA
ITGI Japan
Solvay Business School
University of Antwerp Management School
Aldion Consulting Pte. Ltd.
CA
Hewlett-Packard
IBM
ITpreneurs Nederlands BV
LogLogic Inc.
Phoenix Business and Systems Process Inc.
Project Rx Inc.
Symantec Corporation
Wolcott Group LLC
World Pass IT Solutions

TABLE OF CONTENTS

INTRODUCTION

1. INTRODUCTION

OBJECTIVES OF THE GUIDE

The objective of *IT Assurance Guide* is to provide guidance on how to use COBIT to support a variety of IT assurance activities. If the organisation is already using COBIT as a framework for IT governance, it will enable the leverage of COBIT when planning and performing assurance reviews, so that the business, IT and assurance professionals are aligned around a common framework and common objectives.

This guide is designed to enable efficient and effective development of IT assurance initiatives, providing guidance on planning, scoping and executing assurance reviews using a road map based on well-accepted assurance approaches. Guidance is also provided on how the COBIT resources can be used during these stages supported by detailed tests based on COBIT's processes and control objectives. The guidance and suggested tests, like all the COBIT resources, are not intended to be prescriptive, but should be tailored to suit the specific assurance initiative.

This guide is aimed primarily at assurance professionals, but may be of interest to IT professionals and advisors.

SUMMARY OVERVIEW OF COBIT

Control Objectives for Information and related Technology (COBIT) is a comprehensive set of resources that contains all the information organisations need to adopt an IT governance and control framework. COBIT provides good practices across a domain and process framework in a manageable and logical structure to help optimise IT-enabled investments and ensure that IT is successful in delivering against business requirements.

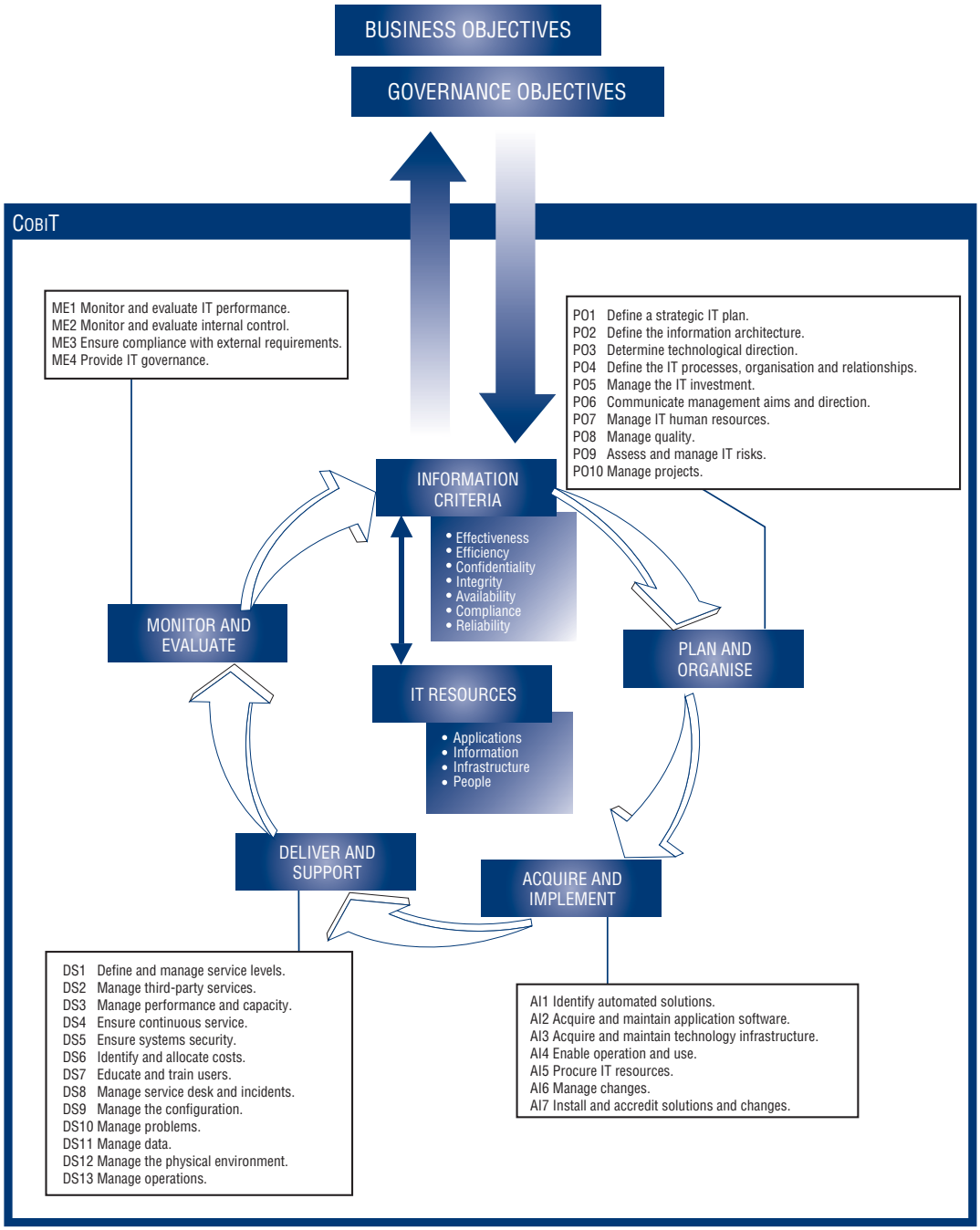
COBIT contributes to enterprise needs by:
- Making a measurable link between the business requirements and IT goals
- Organising IT activities into a generally accepted process model
- Identifying the major IT resources to be leveraged
- Defining the management control objectives to be considered
- Providing tools for management:
  - Goals and metrics to enable IT performance to be measured
  - Maturity models to enable process capability to be benchmarked
  - Responsible, Accountable, Consulted and Informed (RACI) charts to clarify roles and responsibilities

COBIT is focused on what is required to achieve adequate governance, management and control of IT, and is positioned at a high level. COBIT has been aligned and harmonised with other, more detailed IT frameworks, standards and best practices. 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. In this context, the Committee of Sponsoring Organisations of the Treadway Commission (COSO) *Internal Control Framework* and similar compliant frameworks are generally seen as the internal control frameworks for enterprises. COBIT is generally seen as the management and control framework for IT.

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

The COBIT framework is summarised in **figure 1**.

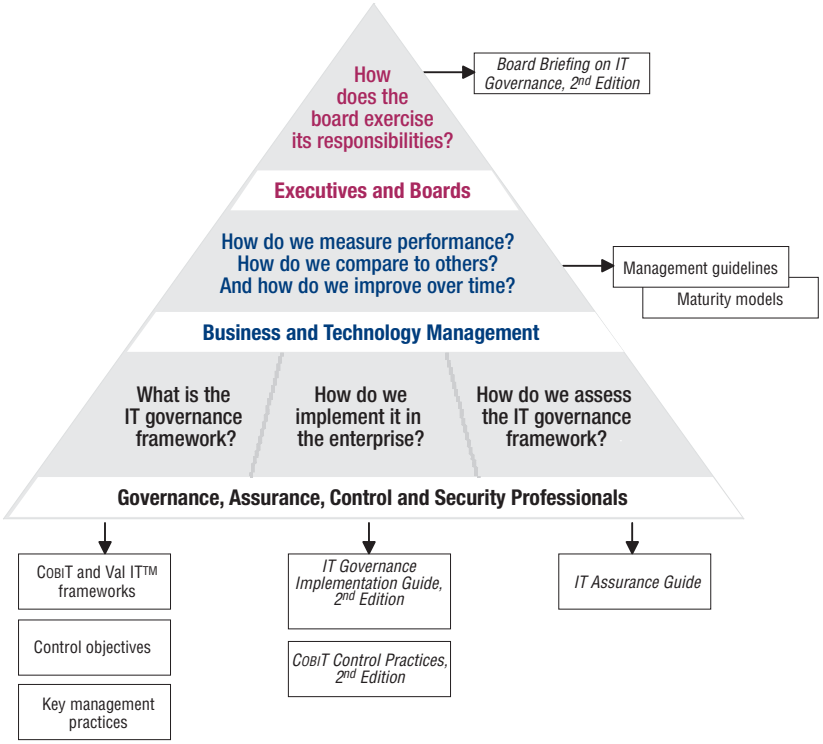
Figure 1—CobiT Framework



The CobiT products have been organised into three levels designed to support:
- Boards of directors and executive management
- Business and IT management
- Governance, assurance, control and security professionals

Figure 2 illustrates the CobiT products within the IT governance body of knowledge aimed at each of these three levels.

Figure 2—Major COBIT-based Products



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).

For more details on each product, see appendix X, COBIT and Related Products. For the most complete and up-to-date information on COBIT and related products, case studies, training opportunities, newsletters and other COBIT-specific information, visit *www.isaca.org/cobit*.

TARGET AUDIENCE

This *IT Assurance Guide* provides detailed guidance for assurance and IT professionals on how COBIT can be used to support a variety of assurance activities for each of the 34 IT processes. Assurance steps and advice are provided for:
- Generic controls that apply to all processes (identified within the COBIT framework by a PCn identifier)
- Application controls (identified within the COBIT framework by an ACn identifier)
- Specific process controls (identified within the COBIT framework by domain identification and process number, e.g., PO6.3, AI4.1)

Assurance steps and guidelines are provided to:
- Test the control design of the control objective
- Test the outcome of the control objective (operational effectiveness)
- Document control weaknesses and their impact

It is assumed that users of this guide are familiar with the concepts of COBIT and have a level of knowledge equivalent to at least the COBIT foundation level (which can be tested online to obtain the COBIT® Foundation Certificate). If this is not the case, it is recommended that the reader undertake the COBIT Foundation Course™. Information on these opportunities is available from *education@isaca.org* and at *www.isaca.org/cobitcampus*.

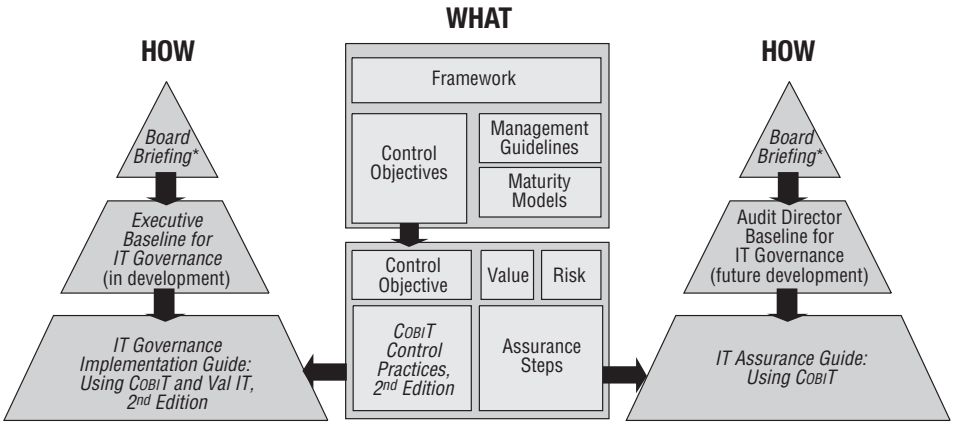
The guide also assumes that the readers are familiar with assurance concepts in general.

COBIT GUIDANCE FOR IT ASSURANCE ACTIVITIES

The COBIT framework, represented in **figure 3**, provides the basis for two guides:
- *IT Governance Implementation Guide: Using COBIT® and Val IT™, 2nd Edition,* which provides a road map and process guidance on how to implement IT governance using the COBIT resources
- *IT Assurance Guide: Using COBIT,* which provides professional guidance for the assurance team and offers a structured assurance approach linked to the COBIT framework that business and IT professionals can understand

As seen in **figure 3**, each guide is fed with different inputs. The *IT Governance Implementation Guide* leverages *COBIT Control Practices*, whilst the *IT Assurance Guide* is based on assurance steps. The two inputs (control practices and assurance steps) are considered mutually exclusive, allowing the guides' users to focus on either part of the IT governance process (implementation or assurance).

Figure 3—Implementation and Assurance Guides



* *Board Briefing on IT Governance, 2nd Edition*

IT Assurance Guide provides assurance advice at different levels. At the process level, process-specific advice is provided on how to test whether control objectives are being achieved and on how to document control weaknesses. At the control objective level, assurance steps are provided to test the control design for each specific control objective based on its control practices. This detailed guidance can be found in appendices I through VI. In chapter 6, Assurance Guidance for COBIT Processes and Controls, some examples can be found on how the detailed guidance can be leveraged for a specific assurance initiative.

At the different levels, generic advice is also provided. Generic advice applies to all processes or control objectives and can be used in addition to, or as an alternative to, the specific advice. These processes are further described in chapter 6.

For the testing steps of the execution stage, this guide provides generic guidance as well as specific, more detailed guidance to assist the IT assurance professional. Generic advice means that it can be applied to any process, control objective or control practice depending on the type of advice. Specific advice refers to advice provided for a specific process, control objective or control practice. An overview of the IT assurance framework that underpins this process is shown in **figure 4**.

COMPONENTS OF *IT ASSURANCE GUIDE*

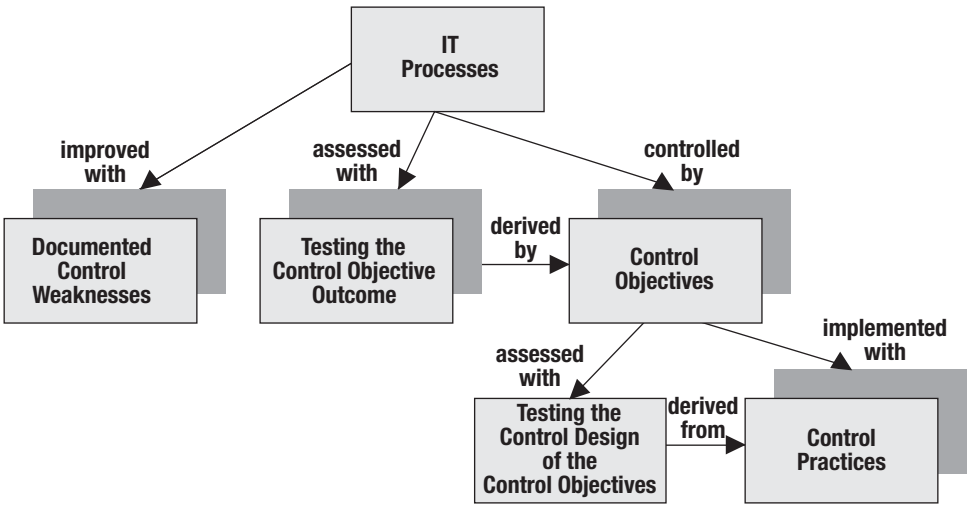
The content of the detailed assurance guidance is organised around the 34 COBIT processes and contains the following components:
- **Control objectives**—Increasingly, organisations are recognising that control of IT is critical for ensuring that IT delivers value to the organisation, risks are managed, regulatory requirements are met, and investments in IT deliver a reasonable return.

  IT control objectives are statements of the desired result or purpose to be achieved by implementing control practices in a particular IT process and often relate directly to specific activities within the process.

  COBIT's control objectives are high-level requirements to be considered for effective control of each IT process. They are written as short, action-oriented management practices. Wherever possible, they follow a logical life cycle sequence.

  Enterprise management has choices relative to control objectives. Members of management should:
  – Select applicable control objectives
  – Balance the investment required to implement management practices required to achieve each control objective with the risk that arises in not achieving it

Figure 4—Overview of the IT Assurance Advice Provided



– Decide which control practices to implement
– Choose how to implement each control practice

CobiT's more than 200 control objectives define what needs to be managed in each IT process to address business requirements and manage risk. They help to define clear policies, foster good practices for IT controls and encourage process ownership. They also provide the reference point for linking good practices to business requirements. Constructed by harmonising more than 40 different control guidance sources, CobiT can be integrated with other standards and practices that focus on specific areas, such as the ISO/IEC 27000 series on information security-related standards, ISO/IEC 9001:2000 Quality Management Systems—Requirements, IT Infrastructure Library (ITIL), *Capability Maturity Model® Integration* (CMMI®), Projects in Controlled Environments 2 (PRINCE2) and *A Guide to the Project Management Body of Knowledge®* (PMBOK®).

- **Value and risk drivers**—Value and risk drivers provide valuable inputs to professionals for use in communicating a business justification for achieving particular control objectives and implementing associated control practices. The value drivers provide examples of the business benefits that can result from good control, whilst the risk drivers provide examples of the risks that may need to be avoided or mitigated. They provide to assurance professionals and IT governance implementors the argument for implementing controls and substantiate the impact of not implementing them.
- **Assurance testing steps**—The assurance testing steps provide guidance at the control objective level for assurance professionals conducting an IT assurance process. The steps are derived from the control practices, which, in turn, are derived from each control objective. The assurance testing steps:
  – Evaluate the design of the controls
  – Confirm that controls are placed in operation
  – Assess the operational effectiveness of the control

  These different testing steps are elaborated in more in detail in chapter 6, Assurance Guidance for CobiT Processes and Controls. Generic assurance steps cover the existence and design effectiveness of the proposed control design as well as the associated responsibilities. Specific assurance steps test the effective operation of controls and are stated at the control objective level. In addition, assurance steps are provided to test the outcomes of control weakness or failure.

  The assurance testing steps are designed to provide the first level of the development of an assurance programme by an internal or external assurance professional. The objective is not to provide a detailed assurance programme that can be used as is and executed. Rather, the intent is for an assurance professional with some experience to use it as the basis for efficiently developing customised assurance programmes that can be used and executed by staff members with less experience. The assurance professional should take the testing steps as a foundation for implementing the assurance initiative. He/she should adjust the testing steps for the reality of the organisation and the objectives of the assurance initiative. The steps are guidance only—they are not a cookbook.

The combination of all assurance components provides a testing method to assist in forming opinions against assurance objectives by combining one or more of the following test types:
- Enquire (via a different source) and confirm.
- Inspect (via walk-through, search, compare and review).

• Observe (i.e., confirmation through observation).
• Reperform or recalculate and analyse (often based on a sample).
• Collect (e.g., sample, trace, extract) and analyse automated evidence.

RELATIONSHIP WITH *COBIT CONTROL PRACTICES*

IT Assurance Guide is part of the COBIT family of products. The assurance test steps have been derived from the *COBIT® Control Practices: Guidance to Achieve Control Objectives for Successful IT Governance, 2nd Edition*, and are expressed in a form usable by assurance professionals for testing activities.

COBIT Control Practices extends the capabilities of the COBIT framework and provides an additional level of detail. The COBIT IT processes, business requirements and control objectives define what needs to be done to implement an effective control structure. *COBIT Control Practices* provides the more detailed guidance at the control objective level on how to achieve the objectives. The control practices consist of the following elements for each of the COBIT control objectives:
• Value and risk drivers, providing 'why do it' guidance
• Control practices to be considered when assessing IT processes and implementing improvements

For each of the control objectives, a list of specific control practices is defined. In addition, three generic control practices are defined, which are applicable to all control objectives. The complete set of generic and specific control practices provides one control approach, consisting of practices that are necessary for achieving the control objective. They provide high-level generic guidance, at a more detailed level under the control objective, for assessing process maturity, considering potential improvements and implementing the controls. They do not describe specific solutions, and further guidance may need to be obtained from specific, relevant standards and best practices, such as ITIL or PRINCE2. The control practices meet the following design criteria in that they:
• Are relevant to the purpose of the control objective
• Can be executed in a timely fashion
• Are realistic and cost-effective
• Are measurable
• Provide for a definition of the roles involved and segregated roles, where appropriate
• Are action-oriented
• Are life-cycle-based, wherever possible

Control practices help ensure that the solutions put forward are more likely to be completely and successfully implemented, by providing guidance on why controls are needed and what the good practices are for meeting specific control objectives.

The control practices are designed to support two audiences:
• Implementors of IT governance (e.g., management, service providers, end users, control professionals)
• Assurance professionals (e.g., internal and external assurance professionals)

For assurance purposes, all the control practices were used to develop detailed assurance steps. The assurance testing steps are designed to provide the first stage of the development of an assurance programme by an internal or external assurance professional. Therefore, professionals using this assurance guide need to take into account that the assurance steps are derived from the control practices. The control practices themselves are not provided in this guide.

The table in **figure 5** provides an overview of the control material that is provided by COBIT and forms the basis for the assurance material in this guide.

Figure 5—Control Objectives and Control Practices

	CONTROL	
	Control Objectives	**Control Practices**
Generic	The COBIT framework provides six process controls that apply to each process. When reviewing a process, these control objectives and the associated practices and assurance steps should be added to the specific control objectives material.	When translating control objectives into practices, the first steps are always the same and cover designing, recording and communicating the approach for achieving the objective, and assigning responsibility and accountability for making it happen.
Specific	For each process, a number of specific control objectives are provided in the COBIT framework.	COBIT provides specific practices for each control objective. Together with the generic practices they provide a control design consisting of the necessary and sufficient steps to achieve the control objective.

The table in **figure 6** describes the assurance material that is derived from the COBIT control material and provided in this guide.

Figure 6—Linking General and Specific Advice to Classes of IT Assurance

	ASSURANCE		
	Testing the Control Design	**Testing Control Process Outcome**	**Documenting Control Weaknesses**
Generic	The generic control practices are translated into assurance steps based on a standard set of assurance methods.	In addition or as an alternative to testing the control design, the outcome of a control objective can be tested. Some standard approaches to looking for evidence are provided that apply to any process.	As an alternative or in addition to the specific advice, some standard approaches to documenting and putting control weaknesses in context are provided, largely focused on identifying comparative data (e.g., benchmarks, measurements, cases).
Specific	The specific control practices are also translated into assurance steps. Combined with the generic practices assurance steps, they provide a complete test of the control design of the objective.	For each process, a number of assurance steps are provided to test the outcome of the control objectives of the process. The generic advice can be used as an alternative or to complement the specific advice.	For each process, specific advice is provided on how to document control weaknesses, relating to the goals, metrics, activities and control objectives of the process.

Finally, additional advice is provided on testing the six application controls (as provided in COBIT), again addressing design, outcome and impact testing.

COBIT, and many of its supporting products, provides detailed support in a wide range of IT assurance activities.

DOCUMENT ROAD MAP

The main sections of this document follow the structure of a suggested IT assurance road map. That road map will be explained in more detail in chapter 2, IT Assurance Principles and Context. The main sections or titles of this road map are:

- Planning
- Scoping
- Execution, including:
  - Refining the understanding of the IT assurance subject
  - Refining the scope of key control objectives
  - Testing the effectiveness of control design
  - Testing the outcomes of key control objectives
  - Documenting the impact of control weaknesses
  - Developing/communicating conclusions and recommendations

Planning is elaborated in chapter 3, Assurance Planning. Scoping is addressed in chapter 4, IT Resource and Control Scoping, and chapter 5, Assurance Initiative Execution, addresses all of the execution steps.

Chapter 6, Assurance Guidelines for COBIT Processes and Controls, explains the structure of the assurance guidance provided for the COBIT processes and control objectives. Chapter 7 explains how COBIT components support IT assurance activities. Appendices I-VI provide the actual assurance tests.

HOW TO USE THIS GUIDE

Even though COBIT has a wide potential audience and can be used by many within an organisation, this guide is particularly intended for internal and external assurance professionals.

A major benefit of this guide is that users can rely on the consistency of the COBIT framework and its related products. The COBIT framework is increasingly being used as an IT governance framework, helping align business and IT management and providing a basis for improving IT's performance. If assurance professionals base their reviews on the same framework as business and IT managers who are improving IT governance and IT performance, everyone involved will be using a common language and it will be easier to agree and implement any necessary control improvements.

This guide can be used by the assurance professional for many different purposes, including:
- Obtaining a view on current good practices on assurance and testing principles
- Learning how using different COBIT components and related concepts can help in planning and scoping assurance initiatives
- Having available a comprehensive reference of all COBIT control objectives and supporting control practices and how they can be tested to obtain assurance that they are effective

IT Assurance Principles and Context

2. IT Assurance Principles and Context

INTRODUCTION

This section describes the overall principles, components and context of IT assurance and explores the IT assurance road map, providing a high-level description of the major steps involved.

The objective of *IT Assurance Guide* is not to provide detailed assurance guidelines. Instead, the objective is to provide high-level guidance on conducting assurance initiatives, and explain briefly a number of fundamental principles for understanding assurance and some related techniques and contributory activities.

Formal standards such as the International Auditing and Assurance Standards Board's (IAASB's) International Framework for Assurance Engagements (IAASB Assurance Framework) may be referenced. However, in this manual, 'assurance' is the term used consistently, as it is broader than the term 'audit'. Assurance also covers evaluation activities not governed by internal and/or external audit standards.

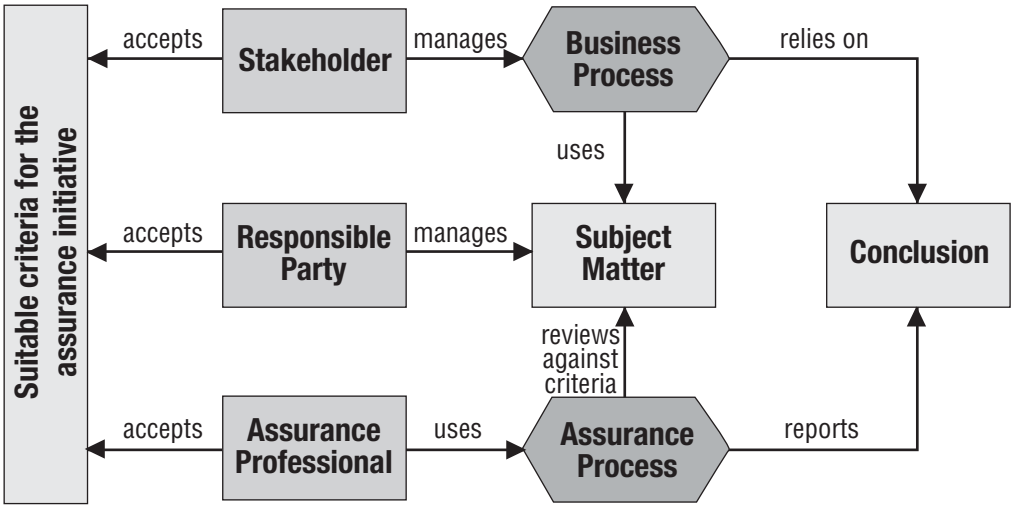
To be called an assurance initiative, five components must be present, as prescribed in the IAASB Assurance Framework and as listed in **figure 7**.

Figure 7—The Five Components of an Assurance Initiative

The objective of an assurance initiative is for an assurance professional to measure or evaluate a subject matter that is the responsibility of another party. For IT assurance initiatives, there is generally also a stakeholder involved who uses the subject matter but who has delegated operation and custodianship of the subject matter to the responsible party. Hence, the stakeholder is the end customer of the evaluation and can approve the criteria of the evaluation with the responsible party and the assurance professional.

The conclusion of the evaluation provides an opinion as to whether the subject matter meets the needs of the stakeholder. **Figure 8** summarises the relationships in an assurance initiative.

Figure 8—Relationships in the Assurance Initiative

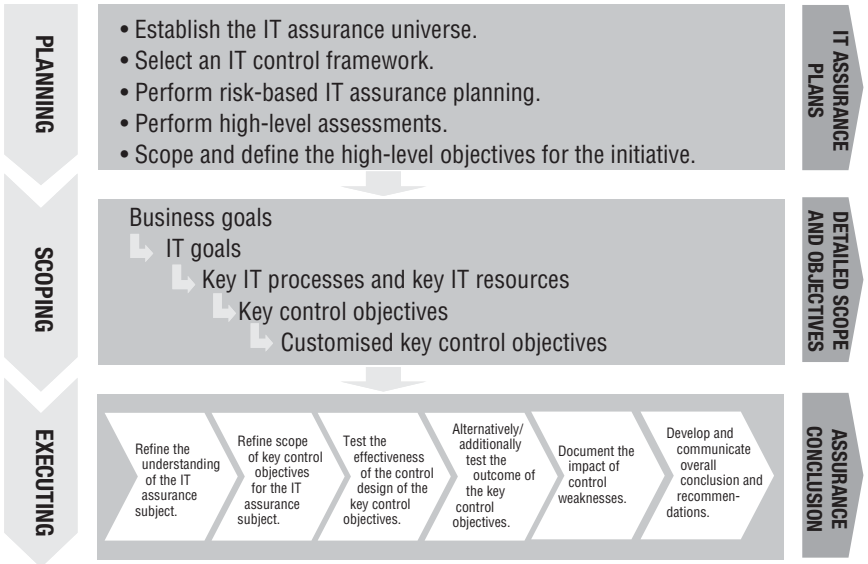


ASSURANCE APPROACH AND ROAD MAP

IT Assurance Road Map

To provide assurance, it is important to follow a consistent methodology or approach. Whilst the specific approach may be unique to each organisation and type of initiative, for the purposes of this guide a fairly common approach is used. It is based on three stages: planning, scoping and execution, with the final stage broken down into six steps. The stages and steps of the road map are presented in **figure 9**.

Figure 9—IT Assurance Road Map



For more significant assurance initiatives, additional information on breaking down the initiative into objectives, actions and deliverables can be found in appendix VIII, IT Scoping. This breakdown provides more detailed guidance that can be applied to IT assurance activity scoping and IT control scoping.

PLANNING

The establishment of the IT assurance universe for the assurance assignment serves as the beginning of every assurance initiative. To create a comprehensive plan, the assurance professional needs to combine an understanding of the IT assurance universe and the selection of an appropriate IT control framework, such as COBIT. The aggregation of these two allows for risk-based planning of the assurance initiative. To set the correct assurance objectives, first a high-level assessment needs to be performed. The end deliverable of this stage is the IT assurance plan (usually annual).

SCOPING

The scoping process can be performed in three different ways:

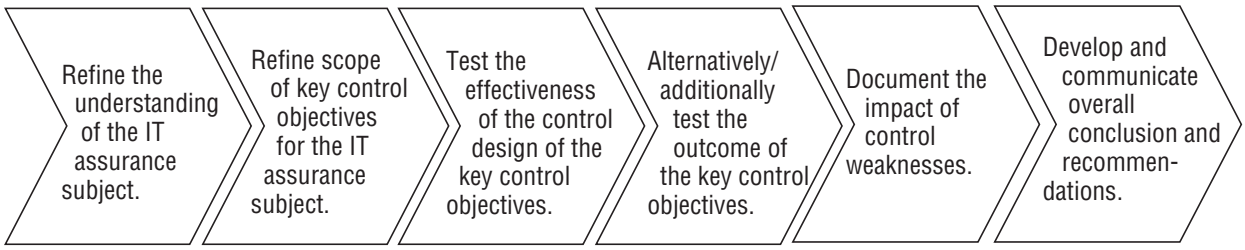
- The most detailed scoping approach starts from defining business and IT goals for the environment under review and identifying a set of IT processes and resources (i.e., assurance universe) required to support those goals. The goals that are subject to the IT assurance initiative can be scoped down to a lower granularity (i.e., key control objectives customised for the organisation).
- A high-level scoping approach may start from benchmarking research executed by ITGI, providing generic guidelines on the relationship of business goals, IT goals and IT processes, as described in COBIT. This generic cascade of goals and processes can be used as a basis for more detailed scoping, as required for the specific environment being assessed.
- A hybrid scoping approach combines the detailed and high-level methods. This approach starts from the generic cascade of goals and processes, but is adapted and modified to the specific environment before continuing the scoping to more detailed levels.

The end deliverables of this stage are the scope and objectives of the different IT assurance initiatives.

EXECUTION

The third stage of the IT assurance road map is the execution stage. **Figure 10** describes an approach that assurance professionals can follow as they execute a particular assurance initiative. These steps cover the core testing activities that the assurance professional executes. Chapter 5, Assurance Initiative Execution, describes each of the steps in more detail. The end deliverable of this stage is the conclusion of the individual IT assurance initiative.

Figure 10—Execution Road Map



IT Assurance Activities

The approach presented in the previous section, IT Assurance Road Map, describes the stages and steps for providing assurance services and provides the structure for this guide. Some of the typical IT assurance activities that may be performed under each of these assurance approach stages are listed in **figure 11**.

Figure 11 introduces the typical assurance activities that can be used—and for which advice is provided—in the different stages and steps of the IT assurance road map. Sometimes the step is the activity; sometimes an activity can be leveraged in several steps.

Figure 11—IT Assurance Activities

- Plan:
  - Perform a quick risk assessment.
  - Assess threat, vulnerability and business impact.
  - Diagnose operational and project risk.
  - Plan risk-based assurance initiatives.
  - Identify critical IT processes based on value drivers.
  - Assess process maturity.
- Scope:
  - Scope and plan assurance initiatives.
  - Select the control objectives for critical processes.
  - Customise control objectives.
- Execute:
  1. Refine the understanding of the IT assurance subject:
     - Identify/confirm critical IT processes.
     - Self-assess process maturity.
  2. Refine the scope of the key control objectives for the IT assurance subject:
     - Update the control objective selection.
     - Customise control objectives.
     - Build a detailed audit programme.
  3. Test the effectiveness of the control design of the key control objectives:
     - Test and evaluate controls.
     - Update/assess process maturity.
  4. Test the outcome of the key control objectives:
     - Self-assess controls.
     - Test and evaluate controls.
  5. Document the impact of control weaknesses:
     - Diagnose residual operational and/or project risk.
     - Substantiate risk.
  6. Develop and communicate overall conclusion and recommendations:
     - Report assurance conclusions.

Whilst most of the advice in this guide focuses on the execution stage of the road map in **figure 12** and Chapter 7, How CobiT Components Support IT Assurance Activities, additional advice is provided for the assurance activities listed, by identifying the CobiT components that can provide a particular benefit for each of these activities. All IT assurance initiatives include most of these activities; therefore, most of the CobiT components can be leveraged in all types of IT-related assurance initiatives.

Figure 12 demonstrates a linkage between assurance activities and where CobiT components can provide a particular benefit. In addition, chapter 7, How CobiT Components Support IT Assurance Activities, provides suggestions on how the different CobiT components can be leveraged to improve the effectiveness and/or efficiency of different IT assurance activities.

Figure 12—Assurance Activities Linked to CobiT Components

IT Assurance Activities	CobiT Components																
	Control Objectives	*CobiT Control Practices*	Value and Risk Statement	Maturity Model	Maturity Model Attributes	RACI (Key Activities and Responsibilities)	Goals and Outcome Measures	Performance Drivers	Management Awareness Tool	Information Criteria	Process List	*Board Briefing on IT Governance, 2nd Edition*	IT Risk and Control Diagnostics	*CobiT Quickstart*	CobiT Online—Searching and Browsing	CobiT Online—Benchmarking	*IT Control Objectives for Sarbanes-Oxley, 2nd Edition*
Perform a quick risk assessment.			✔	✔		✔	✔	✔	✔				✔	✔	✔		
Assess threat, vulnerability and business impact.			✔			✔	✔	✔							✔		✔
Diagnose operational and/or project risk.			✔			✔	✔	✔	✔				✔		✔		
Plan risk-based assurance initiatives.	✔		✔	✔		✔	✔	✔	✔			✔	✔		✔	✔	✔
Identify critical IT processes based on value drivers.				✔	✔	✔	✔		✔	✔	✔	✔	✔		✔	✔	
Assess process maturity.				✔	✔	✔	✔		✔		✔	✔			✔	✔	
Scope and plan assurance initiatives.						✔	✔			✔	✔		✔		✔		✔
Select the control objectives for critical processes.						✔	✔			✔	✔				✔		✔
Customise control objectives.	✔	✔			✔	✔	✔	✔							✔		✔
Build a detailed assurance programme.	✔	✔		✔		✔	✔						✔		✔		✔
Test and evaluate controls.	✔	✔	✔		✔	✔	✔								✔		✔
Substantiate risk.	✔	✔	✔			✔	✔	✔	✔	✔	✔				✔	✔	✔
Report assurance conclusions.	✔	✔	✔	✔		✔	✔	✔	✔	✔	✔				✔	✔	✔
Self-assess process maturity.	✔	✔		✔		✔	✔	✔	✔				✔		✔		
Self-assess controls.	✔	✔				✔	✔						✔	✔	✔	✔	

Reference to Other Assurance Models

Assurance professionals may be familiar with the standards set by organisations, such as IAASB within the International Federation of Accountants (IFAC). IAASB has defined within its International Standards on Auditing stages of conducting an assurance engagement in the context of the financial statement audit. Whilst these stages are specifically defined for the purposes of financial statement audits, they are consistent with the suggested IT assurance processes in this guide. This is illustrated in **figure 13**.

Figure 13—Correlation of IT Assurance and Assurance Stages

			Assurance Stages (IAASB)						
			Determine the responsible party and intended user of assurance output.	Determine the nature of the subject matter.	Define and agree on evaluation criteria.	Collect evidence.	Assess evidence.	Make judgement.	Report and conclude.
Stages in the Road Map	Planning		✔	✔	✔				
	Scoping				✔				
	Execution	Refine the understanding of the IT assurance subject.	✔	✔	✔				
		Refine the scope of key control objectives.			✔				
		Test the effectiveness of the control design.				✔	✔		
		Test outcomes of key control objectives.				✔	✔		
		Document the impact of control weaknesses.				✔	✔		
		Develop and communicate the overall conclusion and recommendations.						✔	✔

The first two steps of the execution stage refine the analysis of the planning and scoping stages and, therefore, map in the same manner to the IAASB standard. For internal assurance, the planning activity is considered to be the annual plan activity and 'refining the plan' refers to planning aspects of individual assignments; whereas, for external audit, these two levels of planning may happen at the same time.

The suggested approach for IT assurance is to make a clear distinction amongst:
- Testing the design of a control objective
- Testing the outcome of a control objective
- Documenting the impact of the weaknesses identified

Each of these three steps deals with collecting and assessing evidence, but in a different manner.

Type of Assurance Advice Provided

For the testing steps of the execution stage, this guide provides generic guidance as well as more specific advice to assist the IT assurance professional, as shown in **figure 14**. The graphic summarises relationships amongst the key CobiT components (process, control objective and control practice) with the steps in the IT assurance road map.

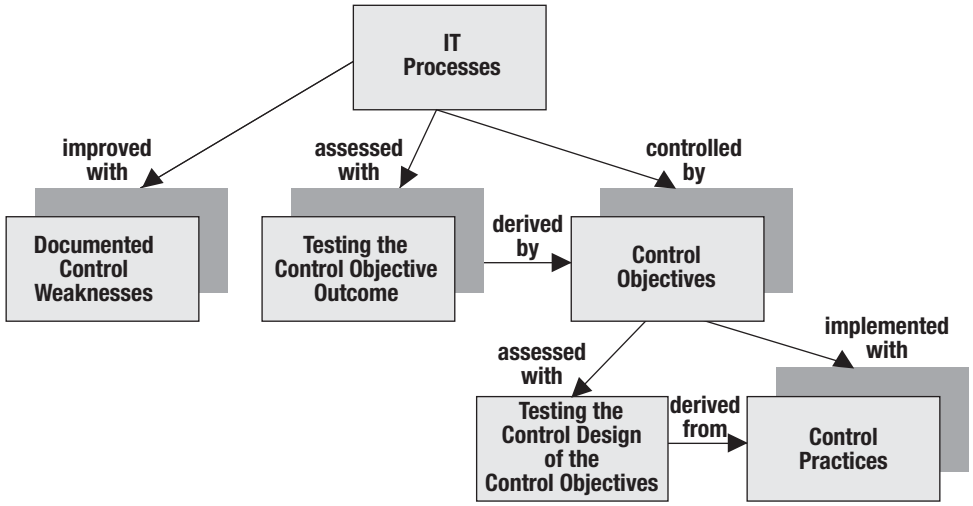
Generic advice means that it can be applied to any process, control objective or control practice depending on the type of advice. Specific advice refers to advice provided for a specific process, control objective or control practice.

The Historical Context—Statutory Audit (Financial Statement Audit)

It is important to understand that, historically, IT assurance started in support of financial statement audits. This class of assurance is still of great relevance, especially in light of the US Sarbanes-Oxley Act and similar regulations internationally.

The purpose of a financial audit is, typically, to express an opinion on financial statements, notably in respect of the following assertions:
- Existence or occurrence of the assets/liabilities/transactions reflected in the financial statements
- Completeness of all financial information presented
- Rights, obligations and relevant commitments appropriately presented in the financial statements
- Valuation or allocation of the value of financial statement captions on a fair and consistent basis
- Presentation and disclosure of values in the appropriate captions of the financial statements and relevant accounting principles or additional information to help ensure correct interpretation

Figure 14—Types of Advice Provided in This Guide



Generic ( ) and Specific ( ) Advice in the Assurance Guide

Together, these assertions, when met, allow the auditor to form and report an opinion on the financial condition of the related entity.

RELEVANT GENERAL STANDARDS AND GUIDANCE

Current recognised guidelines for the external financial statement audit process are embodied in the International Standards on Auditing (ISA).[1]

ISA 315 sets out the requirements of the assurance professional to obtain an understanding of internal control relevant to the audit, which includes the following components:
- The control environment
- The entity's risk assessment process
- The information system, including the related business processes relevant to financial reporting, and communication
- Control activities
- Monitoring of controls

The ISA recognises that, generally speaking, IT provides potential benefits of effectiveness and efficiency for an entity's internal control, but also that it poses specific risks.

With respect to IT, the financial statement assertions can be translated into the following information processing objectives:
- Completeness
- Accuracy
- Validity
- Restricted access

The minimum requirement for the assurance professional is to understand the information systems underpinning business processes relevant for financial reporting and how the entity has responded to risks arising from IT. Since the use of IT affects the way control activities are implemented in the business and related financial reporting, the assurance professional needs to consider whether the entity has responded adequately to the risks arising from IT by establishing effective general IT controls and application controls.

The ISA define general IT controls as policies and procedures that relate to many applications and support the effective functioning of application controls by helping to ensure the continued proper operation of information systems. General IT controls are categorised in the ISA as follows:
- Data centre and network operations
- System software acquisition, change and maintenance

[1] International Standards on Auditing (ISA) are professional standards for the performance of financial audit of financial information. These standards are issued by International Federation of Accountants (IFAC) and cover respective responsibilities, audit planning, internal control, audit evidence, using work of other experts, audit conclusions and audit report, and specialised areas.

• Access security
• Application system acquisition, development and maintenance

ISA 330 gives guidance on the nature, timing and extent of audit procedures to be adopted in response to identified risks. Some specific requirements are set out in the ISA in relation to internal controls validation, including the following:
• When the assurance professional's assessment of risks of material misstatement at the assertion level includes an expectation that controls are operating effectively, the assurance professional should perform tests of controls to obtain sufficient appropriate audit evidence that the controls were operating effectively at relevant times during the period under audit.
• When the assurance professional has determined that it is not possible or practicable to reduce the risks of material misstatement at the assertion level to an acceptably low level with audit evidence obtained only from substantive procedures, the assurance professional should perform tests of relevant controls to obtain audit evidence about their operating effectiveness.

The ISA also specify on the type of procedures to be carried out, stating that, 'the assurance professional should perform other audit procedures in combination with inquiry to test the operating effectiveness of controls'.

RELEVANCE FOR IT ASSURANCE

Specifically in relation to IT, the ISA state that the assurance professional considers the need to obtain audit evidence supporting the effective operation of controls directly related to the assertions, as well as other indirect controls on which these controls depend, such as underlying general IT controls. For that purpose, the CobiT framework provides abundant guidance, and this guide provides an assurance approach that is in line with ISA guidance.

Because of the inherent consistency of IT processing, audit evidence about the implementation of an automated application control, when considered in combination with assurance evidence obtained regarding the operating effectiveness of the entity's general controls (and in particular system development life cycle controls, including change controls) may provide substantial assurance evidence about its operating effectiveness during the relevant period. More guidance on these aspects is provided in chapter 6, Assurance Guidance for CobiT Processes and Controls.

Materiality

When conducting or supporting financial statement audits, assurance professionals ordinarily measure materiality in monetary terms, since what they are auditing is also measured and reported in monetary terms. IT assurance professionals may conduct assurance on non-financial items and, therefore, alternative measures are required. With respect to a specific control objective, a material control is a control or group of controls without which control procedures do not provide reasonable assurance that the control objective will be met.

ISACA IS Auditing Guideline G6 (*www.isaca.org/standard/guideline.htm*) specifies that where the IT assurance objective relates to systems or operations processing financial transactions, the value of the assets controlled by the system(s) or the value of transactions processed per day/week/month/year should be considered in assessing materiality.

For systems and operations not affecting financial transactions, the following are examples of measures that should be considered to assess materiality:
• Criticality of the business processes supported by the system or operation
• Cost of the system or operation (i.e., hardware, software, staff, third-party services, overheads, a combination of these)
• Potential cost of errors (possibly in terms of lost sales, warranty claims, irrecoverable development costs, cost of publicity required for warnings, rectification costs, health and safety costs, unnecessarily high costs of production, high wastage, etc.)
• Number of accesses/transactions/inquiries processed per period
• Nature, timing and extent of reports prepared and files maintained
• Nature and quantities of materials handled (e.g., where inventory movements are recorded without values)
• Service level agreement (SLA) requirements and cost of potential penalties
• Penalties for failure to comply with legal and contractual requirements

Assurance Risk

Assurance risk is the risk that an incorrect opinion is reported by the assurance professional in the presence of material misstatement of the subject matter. Assurance risk is a function of the risk of material error and the risk that the assurance professional will not detect associated errors or control failures.

The risk of material error has two components:

- **Inherent risk**—The susceptibility of an assertion by the responsible party to a misstatement that could be material, individually or when aggregated with other misstatements, assuming that there were no related internal controls[2]
- **Control risk**—The risk that a misstatement that could occur in an assertion and that could be material, individually or when aggregated with other misstatements, will not be prevented or detected and corrected on a timely basis by the entity's internal control

Detective risk is the risk that the assurance professional's procedures will not detect a misstatement that exists in an assertion that could be material, individually or when aggregated with other misstatements. It is important when planning an assurance initiative to assess assurance risk and design an approach to ensure that the assurance objectives are met.

[2] These definitions are drawn from the International Accounting and Assurance Standards Board.

Assurance Planning

3. ASSURANCE PLANNING

INTRODUCTION

The first phase of the IT assurance framework (illustrated in **figure 9**) is the planning phase. Before beginning an assurance initiative, the work of the IT assurance professional should be planned in a manner appropriate for meeting the assurance objectives. For an internal assurance function, the assurance plan should be developed/updated/reviewed at least annually. The plan should act as a framework for assurance activities and serve to address responsibilities set by the assurance charter. For an external IT assurance initiative, a plan should normally be prepared for each initiative. Each type of assurance plan should clearly document the objectives of the initiative and reflect the intended user's strategy and priorities.

As part of the planning process, IT assurance professionals should obtain a good understanding of the assurance universe and the organisation's business goals for IT, IT goals, and how they are planned to be realised through IT processes and IT resources. The extent of the knowledge required is determined by the nature of the organisation, its environment, risks and the objectives of the assurance initiative. To execute the assurance initiative and assurance planning work according to a standardised and structured approach, the IT assurance professional should also identify appropriate control frameworks that could be useful for the assurance initiatives (e.g., COSO, COBIT) or IT management frameworks or standards (e.g., ITIL, ISO/IEC 27000).

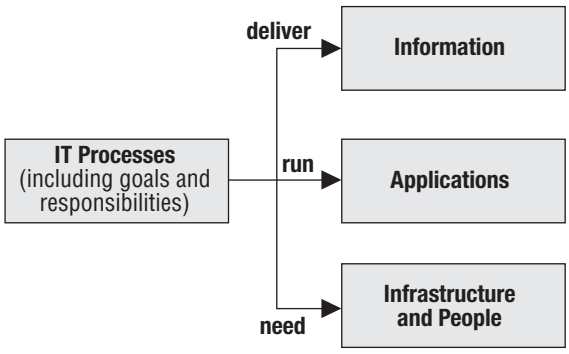
IT ASSURANCE UNIVERSE

The IT assurance universe defines the area of responsibility of the IT assurance provider; it is usually based on a high-level structure that classifies and relates IT processes, resources, risks and controls, allowing for a risk-based selection of discrete IT assurance initiatives. The assurance universe needs to be defined at the enterprise level and must be composed of subjects, units, processes, procedures, systems, etc., that are capable of being defined and evaluated. The building blocks of the assurance universe are units under which assurance can be conducted. For the purpose of *IT Assurance Guide,* COBIT provides a structure to define the IT assurance universe built around the four types of IT resources and 34 IT processes categorised into four domains. The four domains cover the traditional responsibilities in IT of plan, build, run and monitor.

The IT resources identified in COBIT are defined as follows:
- **Applications**—The automated user systems and manual procedures that process the information
- **Information**—The data input, processed and output by the information systems, in whatever form is used by the business
- **Infrastructure**—The technology and facilities (i.e., hardware, operating systems, database management systems, networking, multimedia, etc., and the environment that houses and supports them) that enable the processing of the applications
- **People**—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.

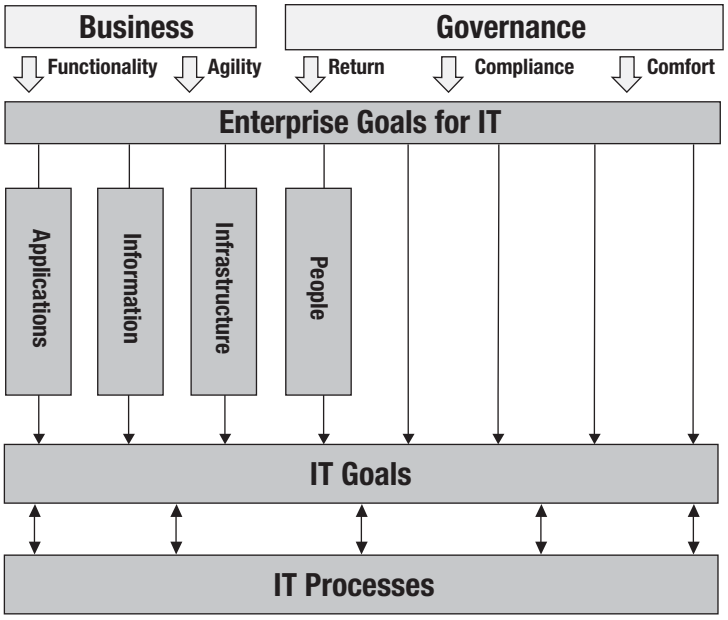
The four domains defined by COBIT are Plan and Organise, Acquire and Implement, Deliver and Support, and Monitor and Evaluate. As shown in **figure 15**, IT processes deliver information to the business, run the applications, and need infrastructure and people. Together, they constitute the enterprise architecture for IT.

Figure 15–Enterprise Architecture for IT



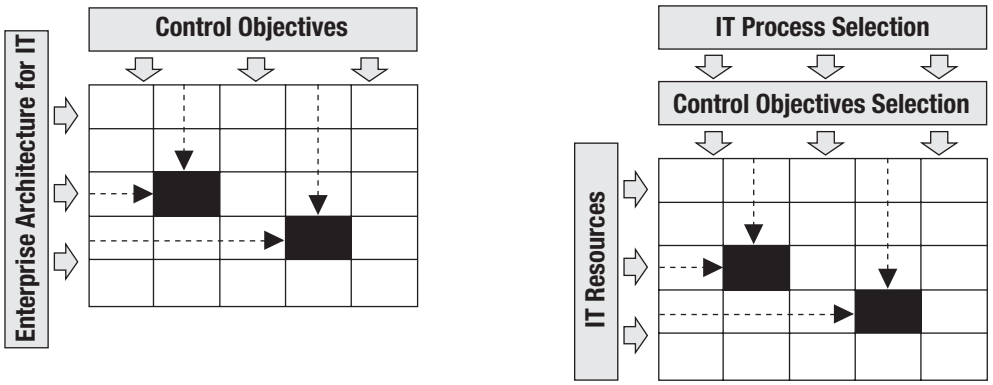
The portfolio of assurance activities within the assurance universe needs to be prioritised by risk level, technological complexity, time since the most recent assurance initiative, strategic importance, age in technology, known control weaknesses, etc. By doing so, assurance resources can be assigned to the units carrying the highest risk for the organisation. The prioritisation is driven by business and governance objectives (regarding functionality, agility, return, compliance and comfort), implying specific value and risk drivers, as illustrated in **figure 16**. This figure also illustrates that it helps to think in terms of IT resources for translating business goals into IT goals (i.e., in terms of the services and information required) and in terms of the infrastructure and people resources required to provide and support the services and information needed. CobiT provides tables of generically applicable enterprise and IT goals that can—after adaptation to the situation at hand—help in determining the subjects in the assurance universe that need the most attention.

Figure 16–Business and IT Goals as Drivers for Assurance Planning



The assurance universe resulting from the analysis work described previously results in most cases in a two-dimensional matrix, with one dimension describing the relevant elements from the enterprise architecture for IT and the other dimension indicating the possible control objectives, as shown in the left part of **figure 17**.

Figure 17–Linking the Enterprise Architecture and Control Objectives



Because the recommended framework is CobiT, with its process structure, a first step in scoping the assurance initiative can consist of selecting the processes, thereby reducing the control objectives in scope on the horizontal dimension. This also allows for simplifying the vertical dimension by concentrating on the IT resources because the processes have been dealt with in the horizontal control objective dimension. This then produces the right side of **figure 17**. If other control frameworks are used that are not process-oriented, the processes need to be retained in the vertical dimension. But even then, most frameworks can be mapped to CobiT (see *www.isaca.org/cobit*) so that after mapping the simplified version can be used.

Other forms of representing the assurance universe are possible. Whatever representation is chosen, balance between completeness, consistency and manageability has to be preserved. Through the proposed technique, all relevant units can be identified and described. Some examples are:

- Applications can either be grouped (in line with the major business processes they support, e.g., sales, logistics, administration, manufacturing, human resources) or listed individually; one can then identify a subset of the IT processes and control objectives to the applications to identify (e.g., an assurance initiative on applications) the development cycle or portfolio management. Projects, which are very often reviewed through project assurance initiatives, can be considered as applications in the making.
- People and the way they are organised (i.e., organisational units) are part of the assurance universe horizontal dimension, allowing, for example, assurance on organisational entities.
- Infrastructure elements (e.g., data centre, networks, IT platforms) are another horizontal dimension, allowing identification of, for example, security reviews of operating systems and networks, or physical reviews of data centres.
- Information includes databases, master files and transaction logs.

Specific topics currently high on the agenda of many IT departments include outsourcing projects and a variety of compliance requirements. Through the process dimension of the assurance universe, the assurance professional can identify the relevant IT processes that manage outsourced IT services, for example, DS1 *Define and manage service levels* and DS2 *Manage third-party services*. By doing so, this specific topic can be included in the overall assurance universe.

RISK-BASED ASSURANCE PLANNING

The assurance professional should use an appropriate risk assessment technique or approach in developing the overall plan for the effective allocation of IT assurance resources. Risk assessment is a technique used to examine units in the assurance universe and select those areas for review that have the greatest risk exposure. The risks associated with each IT layer cannot be determined by reviewing the IT-related risks in isolation, but must be considered in conjunction with the organisation's processes and objectives.

Risk has two major attributes (probability and impact) and has a complex relationship amongst the attributes of the objects involved, which are:

- **Asset**—Something of value (tangible or intangible) worth protecting
- **Threat**—Any situation or event that has the potential to harm a system
- **Threat agent**—Methods and things used to exploit a vulnerability (e.g., determination, capability, motive, resources)
- **Threat event**—An instance of a threat acting upon a system vulnerability in which the system is adversely affected
- **Vulnerability**—A weakness that could be exploited by a threat (e.g., an open firewall port, a password that is never changed, a flammable carpet). A missing control is also considered a vulnerability.
- **Countermeasure**—A synonym for control. The term 'countermeasure' can be used to refer to any type of control, but it is most often used when referring to measures that increase resilience, fault tolerance or reliability of an IT service.
- **Risk**—The potential that a given threat will exploit vulnerabilities of an asset to cause loss or damage to the asset
- **Residual risk**—The risk associated with an event when the control is in place to reduce the effect or likelihood of that event being taken into account

Figure 18 provides the relationship amongst the different components and the major attributes of each. These attributes are essential to analyse the contribution of each component to the risk analysis process. A suggested approach for this process is provided in **figure 19**.

The suggested risk analysis approach starts from the valuation of assets, which in the CobiT framework consists of the information that has the required criteria to help achieve the business objectives (including all the resources necessary to produce that information). The next step is the vulnerability analysis, which identifies the vulnerabilities that apply to the assets (e.g., a business process that needs to comply with data privacy, a business product that deals with financial transactions or infrastructure elements) that determine the availability of many information services. The next phase identifies significant threats that may be able to exploit a given vulnerability (e.g., unintentional events such as errors, omissions and accidents; intentional actions such as fraud, hacking or theft). The probability of the threat, the degree of vulnerability and the severity of the impact are combined to develop threat/vulnerability scenarios and assess their risk. This is followed by the selection of countermeasures (controls) and an evaluation of their cost and effectiveness. After considering the impact of implementing selected controls, residual risk can be determined. The conclusion is an action plan after which the cycle can start again.

Figure 18–Relationship and Attributes of the Risk Analysis Components

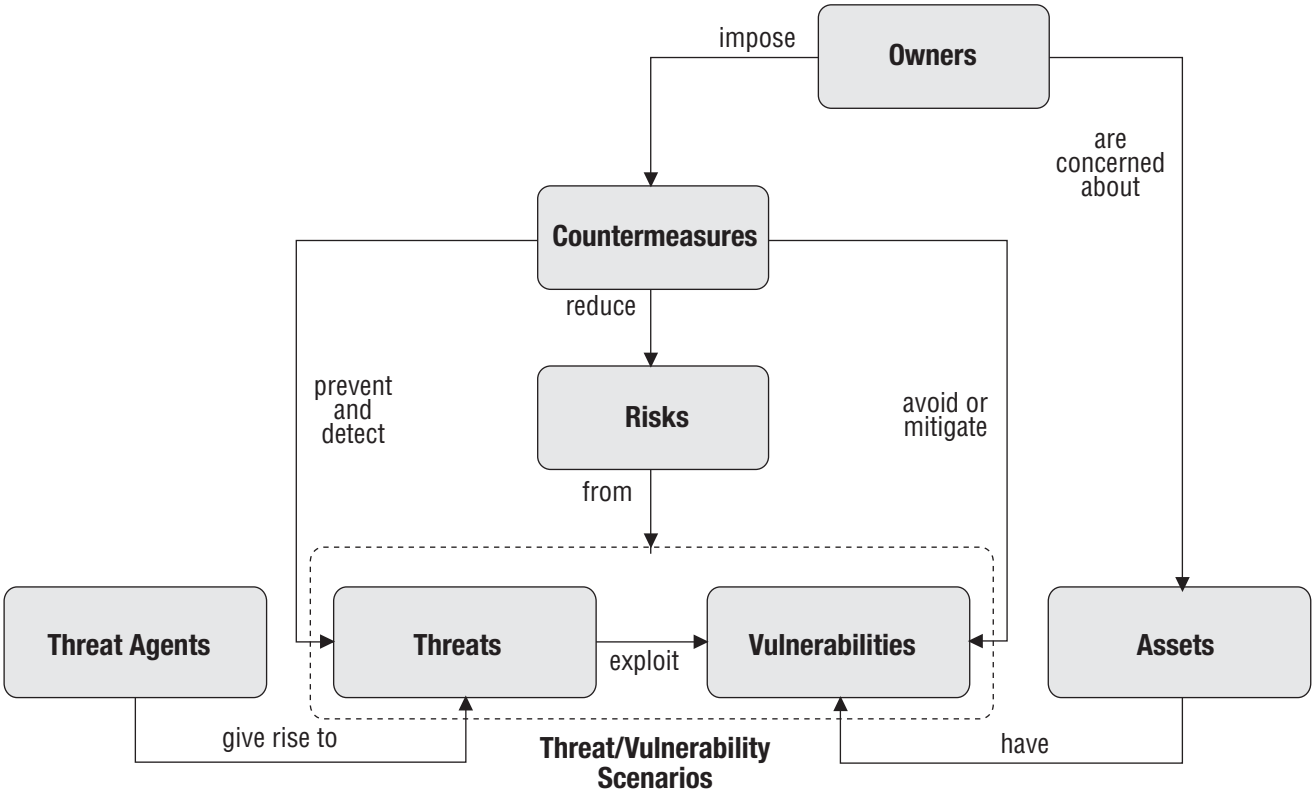
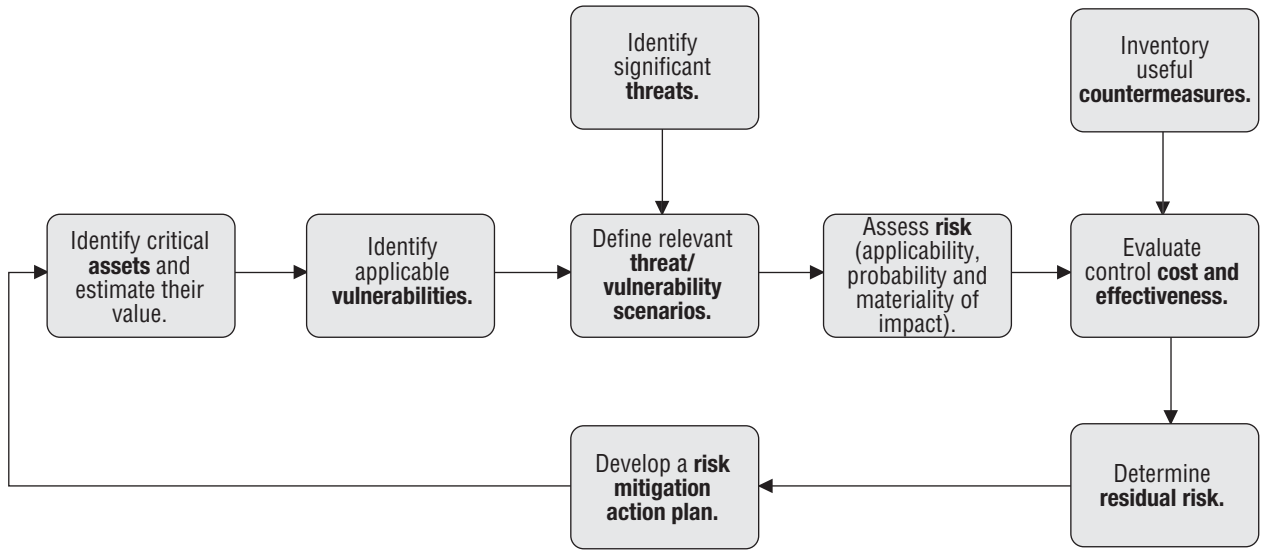


Figure 19—A Risk Analysis Approach Leveraging the Risk Components and Their Attributes



HIGH-LEVEL ASSESSMENTS

High-level assessment can provide support in assurance planning by identifying processes where the maturity/control gap between as-is and to-be is the most significant. Several assessment techniques exist (covering the evaluation against performance and risk attributes, process maturity attributes, control objectives and maturity attributes) resulting in, for example, process compliance profiles as shown in **figure 21**.

The results of such high-level assessment can be used to prioritise the IT assurance work. Specific benefits of such high-level assessments are:
- Making members of IT management aware of their accountability for controlling IT and gaining their buy-in
- High-level checking of compliance with established IT control requirements
- Optimising and prioritising IT assurance resources
- Bridging to IT governance

DEFINE THE SCOPE AND OBJECTIVES OF THE ASSURANCE INITIATIVE

IT assurance professionals should also clearly define the scope and objectives of the assurance work and perform a preliminary assessment of internal control/maturity of the function/activities being reviewed to provide reasonable assurance that all material items will be adequately covered during the assurance initiative.

To execute high-level planning assessments, *COBIT Quickstart* can provide hands-on support (see *www.isaca.org/cobit*). **Figures 20** through **22** also demonstrate other possible templates that can be used for high-level control and maturity assessments. The first template, shown in **figure 20**, is a management awareness diagnostic that evaluates processes against some performance and risk attributes. Completing this template for specific IT processes provides a quick insight into the risks associated (importance and performance), the responsibility (who does it), the formality (documentation), the assurance history and the accountability.

Figure 20—Management Awareness Diagnostic

Importance = How important for the organisation on a scale from 1 (not at all) to 5 (very)
Performance = How well it is done from 1 (very well) to 5 (do not know or badly)
Formality = Is there a contract, an SLA or a clearly documented procedure (**Y**, **N** or ?)
Audited? = **Y**, **N** or ?
Accountable = Name or 'do not know'

Risk		COBIT Processes	Who Does It?						
Importance	Performance		IT	Other	Outside	Do Not Know	Audited?	Formality	Who Is Accountable?
		PO1 Define a strategic IT plan.							
		PO10 Manage projects.							
		AI6 Manage changes.							
		DS2 Manage third-party services.							
		DS5 Ensure systems security.							
		ME1 Monitor and evaluate IT performance.							

The next two templates provide examples of how to execute a process maturity assessment, using the maturity description or maturity attributes. The first template in **figure 21** starts from the process maturity description, which needs to be broken down into several maturity statements. For each of the statements, a compliance value needs to be defined, which enables the IT assurance professional to calculate a 'compliance profile'.

Another approach in assessing process maturity is to leverage the maturity attributes (COBIT maturity models as explained in the COBIT framework). The maturity of a process can be assessed against six maturity attributes:
- Awareness and communication
- Policies, plans and procedures
- Tools and automation
- Skills and expertise
- Responsibility and accountability
- Goal setting and measurement

Figure 21—Assessing the Process Maturity Compliance Profile

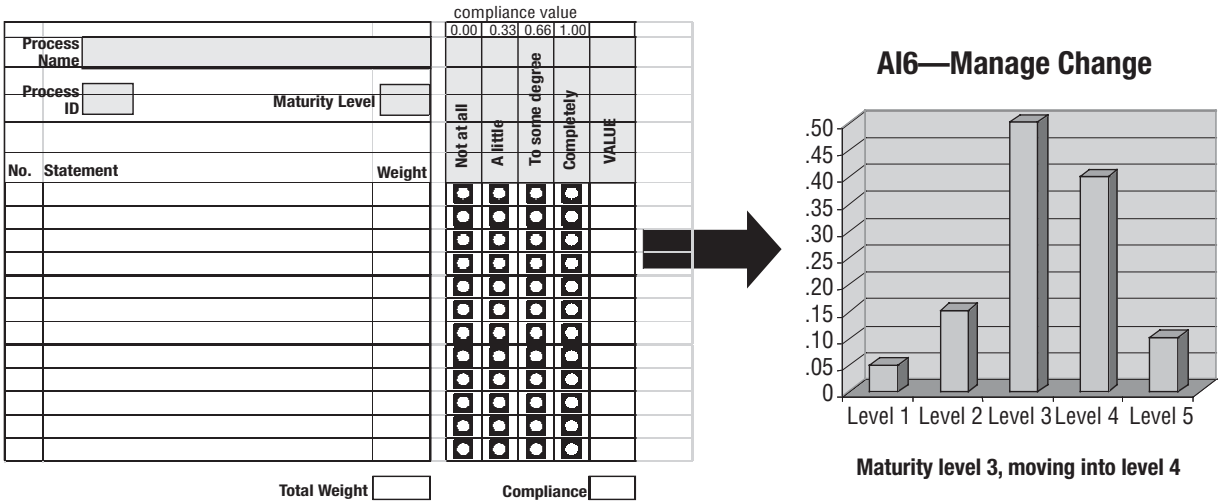


Figure 22—Assessing Process Maturity Attributes

Awareness and Communication	Policies, Plans and Procedures	Tools and Automation	Skills and Expertise	Responsibility and Accountability	Goal Setting and Measurement
5 There is advanced, forward-looking understanding of requirements. Proactive communication of issues based on trends exists, mature are applied, and integrated communication techniques 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 management and to enable end-to-end 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. support improvement of the Tools are being used to 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 concepts and techniques. and use of leading-edge 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.
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.
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 areas are being adopted, as is occasional intuitive application of root cause analysis.
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.
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.

Assessment of these attributes on a template, as shown in **figure 22**, provides the IT assurance professional with a 'rising star scheme', indicating significant gaps between as is and to-be, areas as where attention is needed, and potential quick wins.

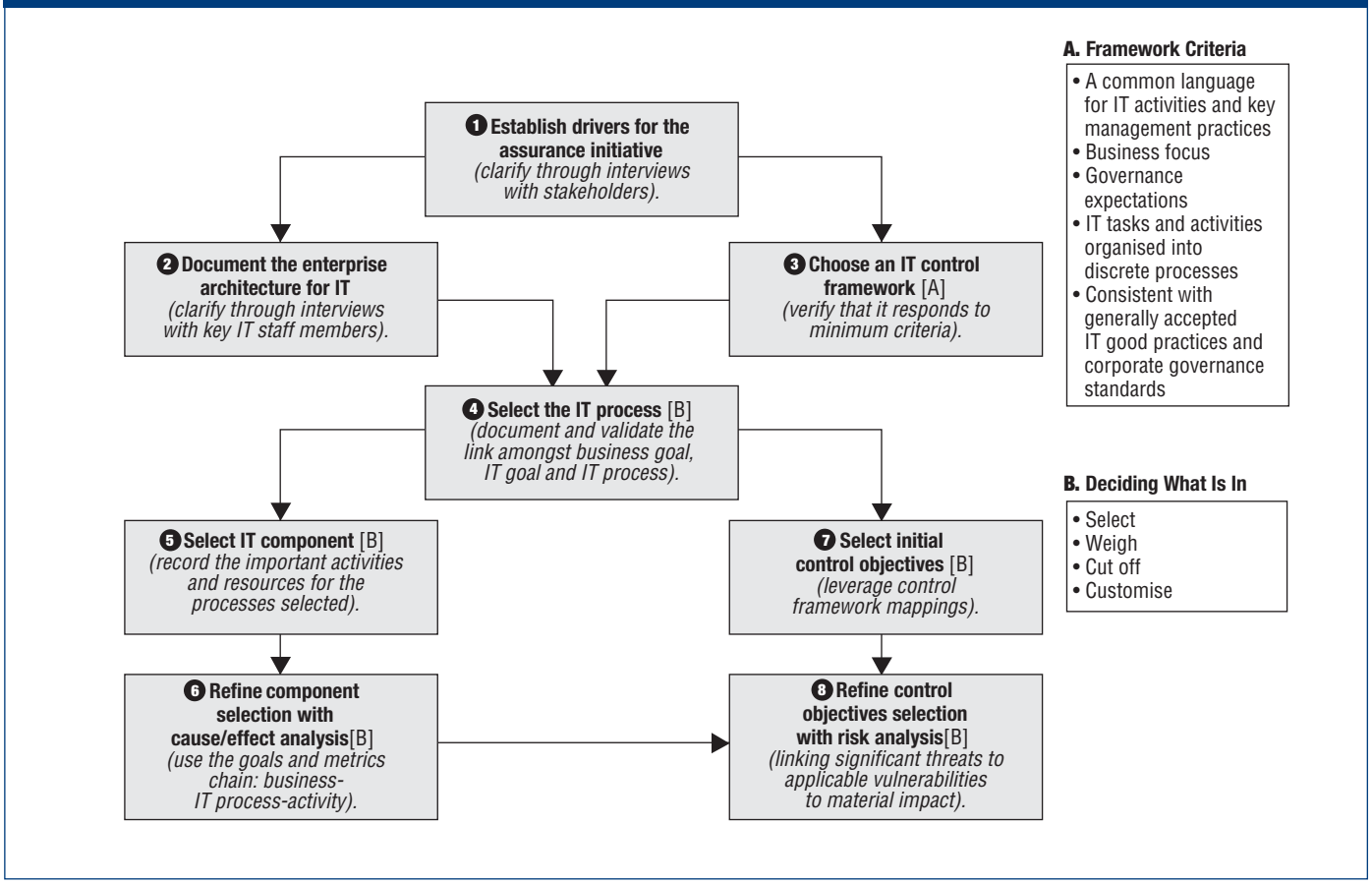
IT Resource and Control Scoping

4. IT RESOURCE AND CONTROL SCOPING

INTRODUCTION

The second stage of the IT assurance framework (illustrated in **figure 23**) is the scoping stage. This stage determines which IT resources and control objectives are covered within a given IT control framework in the execution stage of the initiative. Scoping consists of linking applicable IT resources (e.g., applications, information, infrastructure, people) to applicable IT control objectives and then assessing the materiality of the impact of not achieving a specific control objective. **Figure 23** illustrates the eight-step scoping process.

Figure 23—IT Scoping Road Map



Setting the scope for the initiative too narrowly may result in material factors not being considered. Setting the scope for the initiative too broadly may result in inefficiencies and incorrect conclusions because of limited resources and time. Appendix VIII, IT Scoping, sets out a generic scoping methodology that can be applied to IT assurance initiatives and a variety of other IT governance programmes.

STEPS IN SCOPING IT RESOURCES AND CONTROL OBJECTIVES

Figure 24 describes the eight steps within the scoping phase of conducting the IT assurance initiative. These steps are described in more detail as follows.

Step 1—Establish Drivers for the Assurance Initiative

In the first step, the drivers for the assurance initiative and the corresponding assurance objective are identified. As noted in chapter 1, there are many possible drivers for assurance, including process improvement and meeting compliance needs in support of the financial statement audit. Verifying the drivers for the assurance initiative can be accomplished by activities such as interviewing key stakeholders or inspecting assurance plans or charters.

More specifically, the boundaries of the entity under review need to be unambiguously described, together with the current roles and responsibilities and the resources required by IT to support the defined business needs of the entity under review.

The assurance professional needs to interview appropriate management and staff members to obtain an understanding of:
- Business requirements and associated risks
- Organisation structure
- Roles and responsibilities
- Policies and procedures
- Laws and regulations
- Control measures in place
- Management reporting (status, performance, actions)
- Past issues and corrective actions taken
- Current issues and concerns
- What management hopes to obtain as a result of the assurance initiative

Step 2—Document Enterprise IT Architecture

In the second step, the enterprise IT architecture is documented. The concept and elements of the architecture are set out in chapter 3. The enterprise IT architecture can also be validated by interviews with key IT staff members.

Step 3—Select Control Frameworks

Appropriate control frameworks are selected in the third step. Typically this will be CobiT, but for some initiatives it may be COSO, similar entity-level control frameworks, or more detailed frameworks or standards, such as one of the relevant ISO standards.

Step 4—Identify IT Processes

After the appropriate control framework is chosen, the appropriate IT processes are selected and linked to appropriate IT resources in the next step. IT processes in scope can be identified through analysis of the relationship amongst business goals, IT goals and IT processes.

Step 5—Select IT Components

Step five is described in chapter 2. IT resources are made up of:
- Applications
- Information
- Infrastructure
- People

A number of inputs can be used to determine the IT resources that are relevant to the initiative. The priority here should be on completeness because the subsequent risk analysis determines items that can be excluded from the scope of the initiative. However, efficiency needs to be taken into account as well, to keep the matrix to a reasonable/workable size. The different inputs are:
- **Drivers for the initiative**—The drivers for the assurance initiative are the most important factors for determining the IT components and the control objectives to review. Typical examples are major service breakdown, organisational change and regulatory compliance.
- **Business control requirements**—Given the focus of this guide on IT assurance, it is assumed that the analysis of the required and applicable business controls has occurred so that the scoping of IT controls is limited to how IT supports automated business controls.
- **Enterprise architecture for IT**—The enterprise architecture encompasses the processes involved to deliver the information services, the portfolio of applications and systems in use by the organisation, the technology used to run them, and the people needed to plan, build, operate and support the applications. The relevant IT resources or groups of IT resources can be deduced from the architecture.

Step 6—Refine IT Component Selection

In the initial linking of processes to resources, the assurance professional may derive a rather large portfolio, perhaps broader than can be cost-effectively reviewed within the terms of the assurance initiative. In the sixth step, the assurance professional should refine the selection of IT resources by ensuring that the resources have a direct relationship to the processes relevant to the initiative.

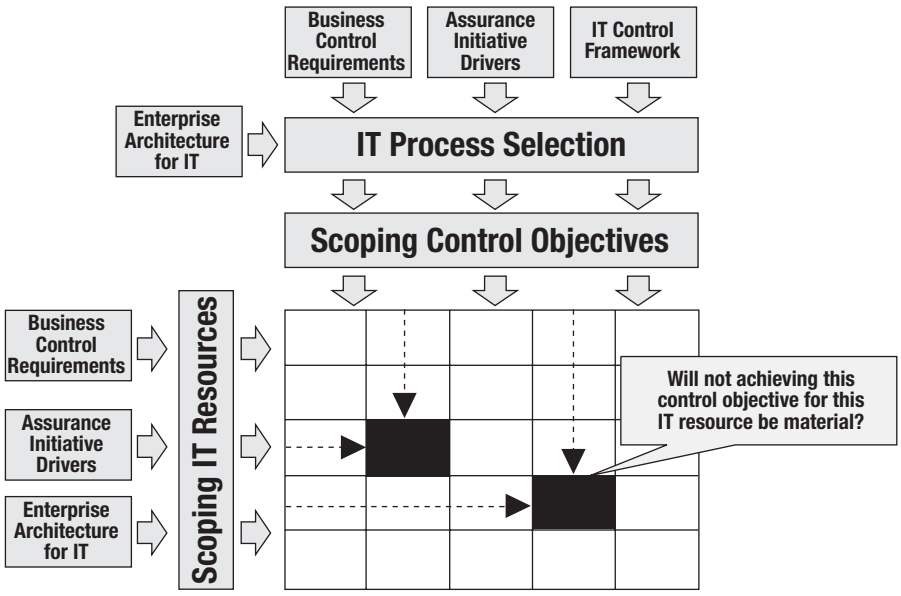
Step 7—Select Control Objectives

The assurance professional makes a first selection of the CobiT control objectives that are relevant for the IT processes that are in scope for the assurance initiative. Often the control objectives need to be customised for the realities of the particular enterprise situation. For most initiatives, scoping IT resources does not require substantial analysis, because it starts from a specific enterprise situation. Conversely, scoping the control objectives needs more analysis because it starts from one or more generic frameworks. CobiT provides material that can support the latter step, by describing a 'risk and value' statement for each of the control objectives, demonstrating why specific controls are needed. Some mapping is required as well as customisation of the selected control objectives to the enterprise environment and the objective of the assurance initiative.

Step 8—Refine Control Objectives Selection

Finally, in the eighth step, the assurance professional links the refined portfolio of IT resources set out in step six to the first cut of control objectives selected in the seventh step. In an iterative process, the professional refines and often reduces the list of control objectives that are relevant for this particular assurance initiative. The process of linking IT resources to control objectives is illustrated in **figure 24**.

Figure 24—Risk-based IT Resource and Control Scoping



In this step, the assurance professional should analyse the risk of not achieving the selected control objectives for the selected IT resources, and retain only the IT resources and control objectives that have a material effect if the control objective is not achieved. The assurance professional should:

- Review the horizontal lines of the matrix (**figure 24**) to determine if there is sufficient risk to keep the IT resource in scope and to identify the resources with high risk that may require more in-depth review and testing
- Review the vertical lines of the matrix (**figure 24**) to remove the control objectives that are low risk and to identify objectives that require enterprisewide solutions as opposed to point solutions

The critical conclusion of this step, illustrated in **figure 24**, is to answer the question, 'Will not achieving this control objective for this class of IT resource be material for this particular assurance initiative?' Only the cells for which the answer is 'yes' should be retained in the final IT control scope.

IT-RELATED BUSINESS GOALS AND IT GOALS

To assist the IT assurance professionals in assurance planning, CobiT provides a detailed cascade from IT-related business goals to IT goals to IT processes. CobiT defines 17 generic business goals, which encompass business drivers and services that directly impact IT. These are translated into supporting IT goals that, in turn, are linked to IT process goals (see appendix 1 in CobiT 4.1). This cascade of business, IT and process goals is particularly useful when analysing the assurance initiative drivers and how they impact the assurance universe.

This cascade of goals can help guide the assurance planning work. As shown in **figure 25**, if the assurance work focuses on a specific business function, IT-related business goals and IT goals can be valuable input for the assurance planning work. Assurance work that focuses on a specific organisational component (e.g., a process) can use IT goals and IT process goals as a source of information for assurance planning.

Figure 25—IT-related Business, IT and IT Process Goals for IT Assurance Planning

		ASSURANCE SUBJECT				
		Business Function	Major Application	Important Infrastructure Component	Organisational Component	Major Change
GOAL INFORMATION	Business Goals	P	S			P
	IT Goals	S	P	P	S	S
	IT Process Goals		S	S	P	S

(P=primary, S=secondary)

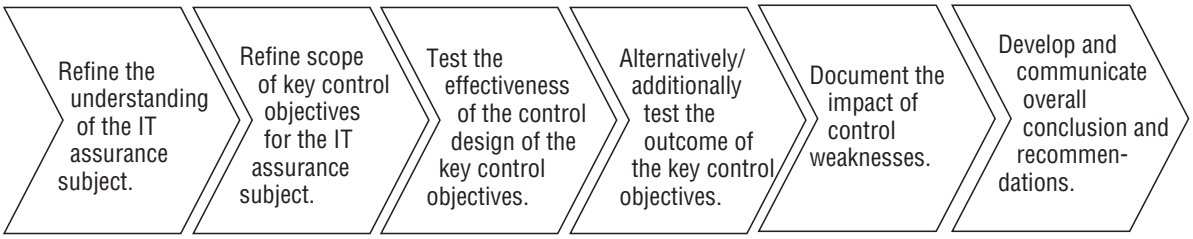
Assurance Initiative Execution

5. ASSURANCE INITIATIVE EXECUTION

INTRODUCTION

The third stage of the IT assurance framework (previously illustrated in **figure 10**) is the execution stage. **Figure 10** describes a road map that assurance professionals can follow as they execute a particular assurance initiative. The remainder of this section will analyse the road map in detail.

Figure 10—Execution Road Map



STEP 1—REFINE UNDERSTANDING

The assurance steps to be performed document the activities underlying the control objectives and identify the stated control measures/procedures in place.

The first step of the execution stage is refining an understanding of the environment in which the testing is performed. This implies understanding the organisation to select the correct assurance scope and objectives. The assurance scope and objectives need to be communicated to and agreed upon by all stakeholders.

The output from this step consists of documented evidence regarding:
- Who performs the task(s), where the task is performed and when the task is performed
- The inputs required to perform the task and the outputs generated by the task
- The stated procedures for performing the task

The assurance professional can structure this step along the following lines:
- Interview and use activity lists and RACI charts.
- Collect and read process description, policies, input/output, issues, meeting minutes, past assurance reports, past assurance recommendations, business reports, etc.
- Prepare the scoping task (objective of process, goals and metrics of process to be reviewed).
- Build an understanding of enterprise IT architecture.

STEP 2—REFINE SCOPE

The assurance steps to be performed determine the scope of the assurance project.

Based on the current and detailed understanding of the IT environment, any revisions that may have been made to the business and/or assurance objectives, and whilst planning a cost-effective testing plan, it may be appropriate to adjust the scope.

The scoping phase performed earlier may, therefore, need to be refined to determine a finalised subset of the assurance universe (e.g., process, system, application) and a set of controls to be reviewed.

Analyse Business and IT Goals

The assurance objectives and approach to the current business objectives should be realigned, and the understanding of business processes, the business goals, and the relevance of IT to the processes and objectives should be updated. The IT goals may need to be adjusted, bearing in mind the latest assurance requirements and the IT organisation.

Select Processes and Controls

The selection of the in-scope IT processes, IT control objectives and IT resources (i.e., applications, information, infrastructure, people) should be refined to establish the assurance boundaries. The selection of the processes, objectives and related resources is performed by assessing if it is likely that non-achievement of the control objective for the IT component will have a material effect.

Analyse Risks

The scope may need to be further adjusted, based on an assessment of the inherent risk of material control objections not being met. This risk-adjusted scope determines the amount of assurance review and testing required.

Finalise Scope

The assurance strategy should be set, and the scope and focus of the assurance approach should be finalised based on the latest understanding of objectives, optimum testing approach and assessed risk, as described previously. The IT processes, IT resources and IT control objectives selection should be adjusted as required by the strategy defined. The documentation required and the testing approach should be determined to ensure the most effective and efficient coverage of assurance objectives.

STEP 3—TEST THE CONTROL DESIGN

This section lists the different techniques that will be used in the detailed assurance steps.

Testing is performed, covering the following main test objectives (also to be found in SAS 70[3] and SysTrust™[4] assurance):
- Evaluate the design of the controls.
- Confirm that controls are placed in operation.
- Assess the operational effectiveness of the controls.

In addition, control efficiency may also be tested.

In the testing phase, different types of testing can be applied. Five generic testing methods include:
- Enquire and confirm:
  - Search for exceptions/deviations and examine them.
  - Investigate unusual or non-routine transactions/events.
  - Check/determine whether something has (not) occurred (sample).
  - Corroborate management statements from independent sources.
  - Interview staff members and assess their knowledge and awareness.
  - Reconcile transactions (e.g., reconciling transactions to bank statements).
  - Ask management questions and obtain answers to confirm findings.
- Inspect:
  - Review plans, policies and procedures.
  - Search audit trails, problem logs, etc.
  - Trace transactions through the process/system.
  - Physically inspect presence (documentation, assets, etc.).
  - Walk through installations, plans, etc.
  - Perform a design or code walk-through.
  - Compare actual with expected findings.
- Observe:
  - Observe and describe the processes.
  - Observe and describe the procedures.
  - Compare actual with expected behaviour.
- Reperform and/or recalculate:
  - Independently develop and estimate the expected outcome.
  - Attempt what is prevented.
  - Reperform what is detected by detective controls.
  - Reperform transactions, control procedures, etc.
  - Recalculate independently.
  - Compare expected value with actual value.
  - Compare actual with expected behaviour.
  - Trace transactions through the process/system.

[3] Statement on Auditing Standards (SAS) No. 70, *Service Organizations*, is an internationally recognised auditing standard developed by the American Institute of Certified Public Accountants (AICPA).
[4] SysTrust is an assurance service developed by the AICPA and the Canadian Institute of Chartered Accountants (CICA).

- Review automated evidenced collection:
  - Collect sample data.
  - Use embedded audit modules.
  - Analyse data using computer-assisted audit techniques (CAATs).
  - Extract exceptions or key transactions.

The assurance steps to be performed assess the adequacy of the design of controls. The following three assurance steps should be performed:
- Observe/inspect and review the control approach, and test the design for completeness, relevancy, timeliness and measurability.
- Enquire whether and confirm that the responsibilities for the control practices and overall accountability have been assigned. Test whether accountability and responsibilities are understood and accepted. Verify that the right skills and the necessary resources are available.
- Enquire through interviews with key staff members involved whether the control mechanism, its purpose, and the accountability and responsibilities are understood.

In summary, the assurance professional must determine whether:
- Documented control processes exist
- Appropriate evidence of control processes exists
- Responsibility and accountability are clear and effective
- Compensating controls exist, where necessary

Additionally and specifically in internal audit assignments, the cost-effectiveness of the control design should be verified with the following assurance steps:
- If the design of the control practice set is effective, investigate whether it can be made more efficient by optimising steps, looking for synergies with other control mechanisms and reconsidering the balance of prevention vs. detection and correction. Consider the effort spent in maintaining the control practices.
- If the control practice set is operating effectively, investigate whether it can be made more cost-effective. Consider analysing performance metrics of the activities associated with this control practice set, automation opportunities and/or skill level.

STEP 4—TEST THE OUTCOME OF THE CONTROL OBJECTIVES

The assurance steps to be performed ensure that the control measures established are working as prescribed, consistently and continuously, and conclude on the appropriateness of the control environment.

To test the outcome or effectiveness of the control, the assurance professional needs to look for direct and indirect evidence of the control's impact on the quality of the process outputs. This implies the direct and indirect substantiation of measurable contribution of the control to the IT, process and activity goals, thereby recording direct and indirect evidence of actually achieving the outcomes as documented in COBIT.

The assurance professional should obtain direct or indirect evidence for selected items/periods to ensure that the control under review is working effectively by applying a selection of testing techniques as presented in step three. The assurance professional should also perform a limited review of the adequacy of the process deliverables and determine the level of substantive testing and additional work needed to provide assurance that the IT process is adequate.

STEP 5—DOCUMENT THE IMPACT OF CONTROL WEAKNESSES

The assurance steps to be performed substantiate the risk of the control objective not being met by using analytical techniques and/or consulting alternative sources.

When control weaknesses are found, they have to be properly documented, taking into account their often sensitive and confidential nature. In addition, particular care is required to correctly analyse and assess the severity of the observed weaknesses and the potential business impact they may have.

The objective of this step is to conduct the necessary testing to provide management with assurance (or non-assurance) about the achievement of a given business process and its related control objectives. More detailed analysis should occur when:
- No control measures are in place
- Controls are not working as expected
- Controls are not consistently applied

This should result in a thorough understanding of the control weaknesses and the resulting threats and vulnerabilities, and an understanding of the potential impact of the control weaknesses.

The following assurance steps can be performed to document the impact of not achieving the control objective:
- Relate the impact of not achieving the control objective to actual cases in the same industry and leverage industry benchmarks.
- Link known performance indicators to known outcomes and, in their absence, link the cause to its effect (cause/effect analysis).
- Illustrate what the impact would affect (e.g., business goals and objectives, enterprise architecture elements, capabilities, resources).
- Illustrate the impact of control weaknesses with numbers and scenarios of errors, inefficiencies and misuse.
- Clarify vulnerabilities and threats that are more likely with controls not operating effectively.
- Document the impact of actual control weaknesses in terms of bottom-line impact, integrity of financial reporting, hours lost in staff time, loss of sales, ability to manage and react to the market, customer and shareholder requirements, etc.
- Point out the consequence of non-compliance with regulatory requirements and contractual agreements.
- Measure the actual impact of disruptions and outages on business processes and objectives, and on customers (e.g., number, effort, downtime, customer satisfaction, cost).
- Document the cost (i.e., customer and financial impact) of errors that could have been caught by effective controls.
- Measure and document the cost of rework (e.g., ratio of rework to normal work) as an efficiency measure affected by control weaknesses.
- Measure the actual business benefits and illustrate cost savings of effective controls after the fact.
- Use benchmarking and survey results to compare the enterprise performance with others.
- Use extensive graphics to illustrate the issues.

COBIT provides support in the following ways:
- The business, IT and process goals and the information criteria in the process descriptions indicate what business values are at risk if controls are not implemented properly.
- For each control objective, there are value and risk driver statements that indicate the benefits to be gained and the risks to be avoided by improving controls.
- The RACI charts demonstrate which roles might be affected by the risk and, therefore, should be informed of the substantive testing outcome.
- Maturity models can be leveraged to benchmark internally and against other industries or competitors in an easy, accessible and understandable manner, helping to influence management. Benchmarking data are available in COBIT Online.

STEP 6—DEVELOP AND REPORT OVERALL CONCLUSION AND RECOMMENDATIONS

The assurance steps to be performed communicate the substantiated risk of the control weaknesses to the different stakeholders of the assurance initiative.

The assurance professional should document any identified control weaknesses and resulting threats and vulnerabilities, and identify and document the actual and potential impact (e.g., through root cause analysis). In addition, the assurance professional may provide comparative information (e.g., through benchmarks) to establish a reference framework in which the test results ought to be evaluated. As potential guidance to this, a generic maturity model for internal control is provided in chapter 7, Maturity Model for Internal Control, 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 objective is to identify items of significance to be able to articulate to the stakeholder the recommended actions and reasons for taking action. This phase includes aggregating the results of the previous phases, developing a conclusion concerning the identified control weaknesses and communicating:
- Recommended actions to mitigate the impact of the control weaknesses
- Performance comparison to standards and best practices for a relative view on the results
- The risk position regarding the process

The formulated conclusion and recommendations should allow the responsible party to take further steps and remedial actions.

When the assurance initiative is performed within an assurance context, the assurance professional needs to be thoughtful of formal assurance communication and compliant with assurance reporting standards and guidelines (available at *www.isaca.org*).

Assurance Guidance for CobiT Processes and Controls

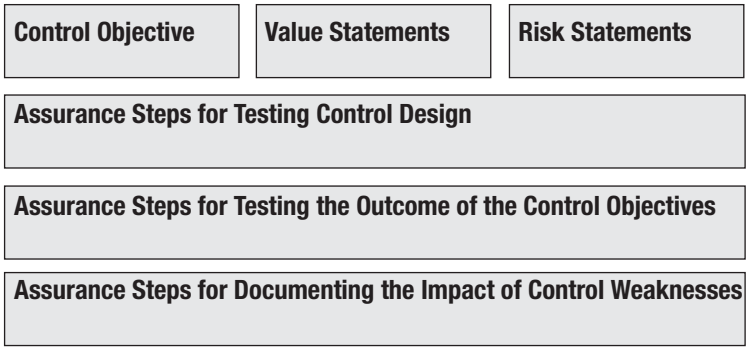
6. ASSURANCE GUIDANCE FOR COBIT PROCESSES AND CONTROLS

INTRODUCTION

This section describes the structure of the detailed testing guidance based on COBIT, covering six generic controls applicable to all IT processes, IT general controls based on the 34 COBIT IT processes and six application controls.

Guidance is provided for testing control design, testing control outcome and documenting the impact in appendices I through VI, according to the layout in **figure 26**.

Figure 26—Structure of the Detailed Assurance Advice in Appendices I to VI



GENERIC PROCESS CONTROLS

Each COBIT process has generic control requirements that are identified by generic process controls within the Process Control (PC) domain (see appendix I). These are applicable for all COBIT processes and should be considered together with the detailed COBIT control objectives to have a complete view of control requirements.

The six generic process controls, detailed in appendix I, Process Control, are:
- PC1 Process goals and objectives
- PC2 Process ownership
- PC3 Process repeatability
- PC4 Roles and responsibilities
- PC5 Policy, plans and procedures
- PC6 Process performance improvement

GENERIC CONTROL PRACTICES

Three generic control practices and, consequently, three generic assurance steps are defined. They are:
- Approach
- Accountability and responsibility
- Communication and understanding

The complete set of generic and specific control practices provides one consistent control approach necessary and sufficient for achieving the stated control objectives. Other control approaches with different sets of practices may exist; hence, there is a need to always verify the appropriateness of the control design at the outset of control implementation or at the outset of assurance activities.

Approach

The generic approach control practice consists of:
- **Generic control practice**—Designs the control approach for achieving this control objective, and defines and maintains the control practices that implement this design
- **Assurance step**—Enquires whether and confirms that a set of practices has been defined to achieve the objective; observes/inspects and reviews the control approach, and tests the design for completeness, relevancy, timeliness and measurability

Accountability and Responsibility

The generic accountability and responsibility control practice consists of:

- **Generic control practice**—Defines and assigns accountability and responsibility for the control objective as a whole, and responsibility for the different control practices (see RACI charts in COBIT); makes sure personnel have the right skills and necessary resources to execute these responsibilities
- **Assurance step**—Enquires whether and confirms that responsibilities for the control practices as well as overall accountability have been assigned in a cost-effective and efficient manner; tests whether accountability and responsibilities are understood and accepted; verifies that the right skills and necessary resources are available

Communication and Understanding

The generic communication and understanding control practice consists of:

- **Generic control practices**—Ensures the control practices, as implemented, address the control objectives and are communicated and understood
- **Assurance step**—Enquires through interviews with key staff members involved whether the control mechanism, its purpose, and the accountability and responsibilities have been communicated and are understood

IT GENERAL CONTROLS

General controls relate to the environment within which automated application systems are developed, maintained and operated and which are, therefore, applicable to all the applications. They ensure the proper development, implementation and maintenance of all automated applications, and the integrity of program and data files and of computer operations.

Guidance is provided on how to test COBIT's 34 IT processes, organised into four appendices (see appendices II-V) based on COBIT's four domains.

APPLICATION CONTROLS

Application controls relate to the transactions and standing data pertaining to each automated application system and are specific to each such application. They ensure the completeness and accuracy of the records and the validity of the entries made in the transactions and standing data resulting from both manual and automated processing. They are defined further in the Application Control (AC) domain in appendix VI.

Relative to IT assurance, a distinction is made between application and general controls. General controls are controls embedded in the IT organisation, its processes and services. Examples include:

- Systems development
- Change management
- Security
- Computer operations

Controls embedded in business process applications, on the other hand, are commonly referred to as application controls. Examples include:

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

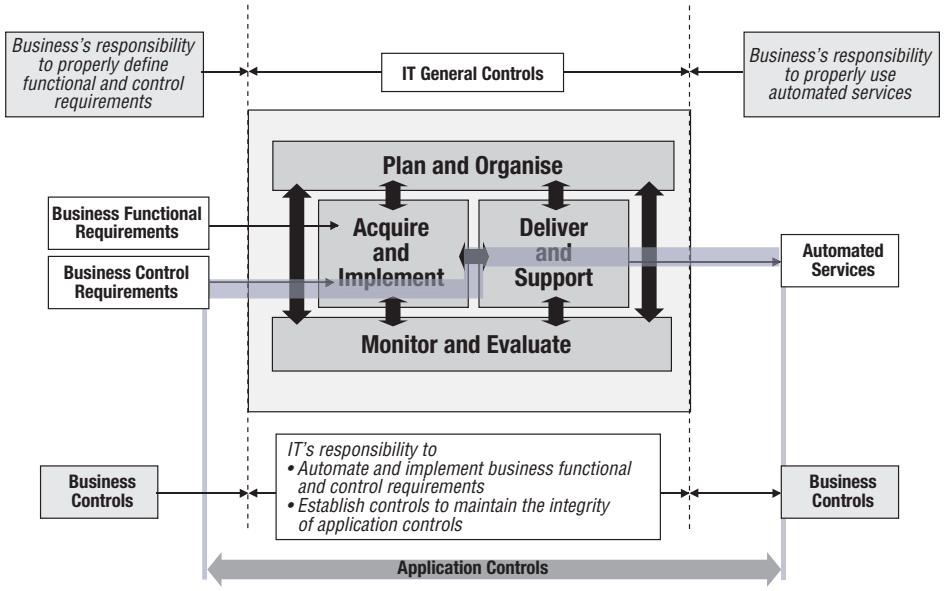
Therefore, the objectives of application controls generally involve ensuring that:

- Data prepared for entry are complete, valid and reliable
- Data are converted to an automated form and entered into the application accurately, completely, and on time
- Data are processed by the application completely and on time, and in accordance with established requirements
- Output is protected from unauthorised modification or damage and distributed in accordance with prescribed policies

COBIT assumes the design and implementation of automated application controls to be the responsibility of IT, covered in the Acquire and Implement (AI) domain, based on business requirements defined using COBIT's information criteria. The operational management and control responsibility for application controls is not with IT, but with the business process owner. IT delivers and supports the applications' services and the supporting information databases and infrastructures. Therefore, the COBIT IT processes cover general IT controls but not application controls, because these are the responsibility of business process owners and, as described previously, are integrated into business processes.

Business controls are not in the scope of COBIT and *IT Assurance Guide*. **Figure 27** sets the boundaries of IT general controls and application controls, delineating at the same time the extent to which COBIT handles business controls.

Figure 27—IT General Controls and Application Controls



For automated services, the business is responsible for defining functional, as well as control, requirements to be included in all business processes supported by applications. Subsequently, IT responsibilities include automation of the business functional and control requirements and establishment of controls to maintain the integrity of the business applications.

Just as for the IT general controls and generic process controls, guidance is provided for testing the design and outcome and documenting impact for each of the six COBIT application controls, detailed in appendix VI, Application Control:
- AC1 Source document preparation and authorisation
- AC2 Source document collection and data entry
- AC3 Accuracy, completeness and authenticity checks
- AC4 Data processing integrity and validity
- AC5 Output review, reconciliation and error handling
- AC6 Transaction authentication and integrity

Application control weaknesses may have an impact on the entity's ability to process business transactions through the impacted business processes and applications. Application controls are a subcomponent of the entity's business controls. Weaknesses in application controls may be mitigated by compensating manual business and organisational control activities. The impact of application control weaknesses should be considered in the context of the underlying business process nature and related transactions and the impact of other business process controls and, as such, should be considered in consultation with the business process assurance provider.

EXAMPLES OF THE USE OF DETAILED ASSURANCE STEPS

Some illustrative examples of how the assurance testing steps could be applied follow.

Example 1—Testing of Control Design

SITUATION

General computer controls are reviewed in a transaction processing organisation with assessment of the process AI6 *Manage changes*, control objective AI6.2 *Impact assessment, prioritisation and authorisation.*

OBSERVATIONS

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

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

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

Example 2—Testing for the Effectiveness of the Control

SITUATION
General computer controls are reviewed in a transaction processing organisation with assessment of the process AI6 *Manage changes*, control objective AI6.3 *Emergency changes.*

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

As part of the control effectiveness testing, a sample of emergency change requests was selected from the change management tool and traced to its reintroduction as normal changes. This tracing included verification of whether the emergency change was actually introduced again as a normal change and whether it was processed following the normal change management procedure.

The assurance professional observed that from the sample of 25 emergency changes selected, three of them were not subsequently reprocessed as normal changes. In addition, the assurance professional found that from the 22 emergency changes that had been duly reintroduced, only 10 were discussed at the change management board—or at least that there was a trace available that indicated that the 10 changes were discussed (trace included information stored in the change management tool).

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

Example 3—Documenting the Impact of Control Weaknesses

SITUATION
General computer controls are reviewed in a transaction processing organisation with assessment of the process AI6 *Manage changes*, control objective AI6.3 *Emergency changes.*

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

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

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

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

How CobiT Components Support IT Assurance Activities

7. How CobiT Components Support IT Assurance Activities

INTRODUCTION

Figure 28 links the list of typical IT assurance activities to the CobiT components that can be leveraged to make the activities more efficient and effective. It demonstrates how CobiT can support specific assurance-related activities, often performed as stand-alone tasks, in addition to how CobiT has provided support to the suggested IT assurance road map, described in the previous sections.

Links have been indicated only where there is specific and strong support for an IT assurance activity. There are some key components, however, that support all activities. In practice, users of CobiT adapt and tailor the CobiT resources for their specific purposes and discover how CobiT can add value to a particular task. The table is, therefore, only a guide.

Two of the most useful components are the goals and outcome measures and the RACI charts (key activities and responsibilities). They capture the essence of IT, its processes, activities and objectives and, hence, support all aspects of planning, scoping and assurance execution. Another important component for IT assurance activities is CobiT Online—its searching and browsing functions enable easier access to all the main CobiT content as well as useful benchmarking data. Those CobiT components important for assurance activities are shaded in **figure 28**.

Figure 28—Linking IT Assurance Activities and CobiT Components

	CobiT Components																
IT Assurance Activities	Control Objectives	*CobiT Control Practices*	Value and Risk Statements	Maturity Model	Maturity Model Attributes	RACI (Key Activities and Responsibilities)	Goals and Outcome Measures	Performance Drivers	Management Awareness Tool	Information Criteria	Process List	*Board Briefing on IT Governance, 2nd Edition*	IT Risk and Control Diagnostics	*CobiT Quickstart*	CobiT Online—Searching and Browsing	CobiT Online—Benchmarking	*IT Control Objectives for Sarbanes-Oxley, 2nd Edition*
Perform a quick risk assessment.			✔	✔		✔	✔	✔	✔				✔	✔	✔		
Assess threat, vulnerability and business impact.			✔			✔	✔	✔							✔		✔
Diagnose operational and project risk.			✔			✔	✔	✔	✔				✔		✔		
Plan risk-based assurance initiatives.	✔		✔	✔		✔	✔	✔	✔			✔	✔		✔	✔	✔
Identify critical IT processes based on value drivers.				✔	✔	✔	✔		✔	✔	✔	✔	✔		✔	✔	
Assess process maturity.				✔	✔	✔	✔		✔		✔	✔			✔	✔	
Scope and plan assurance initiatives.						✔	✔			✔	✔		✔		✔		✔
Select the control objectives for critical processes.						✔	✔			✔	✔				✔		✔
Customise control objectives.	✔	✔			✔	✔	✔	✔							✔		✔
Build a detailed assurance programme.	✔	✔		✔		✔	✔						✔		✔		✔
Test and evaluate controls.	✔	✔	✔		✔	✔	✔								✔		✔
Substantiate risk.	✔	✔	✔			✔	✔	✔	✔	✔	✔				✔	✔	✔
Report assurance conclusions.	✔	✔	✔	✔		✔	✔	✔	✔	✔	✔				✔	✔	✔
Self-assess process maturity.	✔	✔		✔		✔	✔	✔	✔				✔		✔		
Self-assess controls.	✔	✔				✔	✔						✔	✔	✔	✔	

The following sections summarise the most important relationships in **figure 28**, first from the components point of view and then from the activities point of view. To conclude, the strongest links between activities and components are circled in **figure 28**.

CobiT COMPONENTS

Control objectives and practices are mostly useful for testing related activities, although since the control objectives are high-level and similar to key management practices, they can be considered during planning activities. Both are also helpful for the selection and customisation of control objectives for an assurance initiative.

The list of COBIT processes and the domains provide a responsibility structure for IT and help ensure the completeness of the assurance coverage. The list is useful in the planning phase and also when summarising the conclusions of an assurance initiative. Similarly, information criteria provide a generic and simple high-level structure of the objectives of IT processes and are equally useful for structuring assurance plans and conclusions.

Maturity models are very useful tools for high-level assessments of processes, identification of key processes, planning which processes need most attention in the assurance programme and also when summarising the assurance conclusions. The maturity attributes provide more details for process maturity assessment, and because they are generic for all processes, they are also an alternative to the specific process maturity descriptions provided for each COBIT process. Because maturity models describe *how* processes are managed, the detailed attributes can be used to further customise control objectives, which usually describe only *what* needs to be done. Maturity models are increasingly being used by IT management for self-assessment and can, therefore, provide a common approach for both the assurance and IT professionals to understand and agree upon priorities and areas on which to focus attention.

Whereas performance drivers play an important role for assurance activities in the planning and reporting phases of an IT assurance road map, they are also a good source for customising control objectives because they imply that certain actions need to happen or conditions need to exist that will increase the probability of successfully achieving the process's objectives and goals.

Value and risk statements provide the arguments to justify controls but are also primary inputs when performing high-level or detailed risk assessments. They are also starting points when identifying critical processes and IT components.

The management awareness and diagnostic tools are provided in Supplemental Tools and Materials, available online and on CD-ROM with the *IT Governance Implementation Guide: Using COBIT and Val IT, 2nd Edition*. They are tools to perform initial high-level assessments of process importance, significant risks and the state of process controls, typically done in the early stages of the IT assurance initiative.

The assessment form presentation of *COBIT Quickstart* lends itself easily for quick or high-level assessments as well as for efficient self-assessments.

Benchmarking data and functionality as provided in COBIT Online are useful to portray how the entity compares on process management and controls with other enterprises in the same industry, geography or size segment. The comparison is supported with pie chart and spider diagrams. Such benchmarks lend a lot of credibility to the conclusions of assurance activities but can also be used earlier in the assurance life cycle (e.g., to identify processes that need early or in-depth assurance coverage because of gaps with the rest of the industry).

IT ASSURANCE ACTIVITIES

To gain insight into the entity where the IT assurance activities are to be performed, the COBIT components that provide the best support for the assurance professional are the process structure, maturity models, goals, outcome measures and performance drivers.

Risk-based IT assurance planning has become common practice and is well supported by COBIT's maturity modelling and COBIT Online's benchmarking to identify where the highest potential risks are. The risk and value statements of the control objectives provide additional support if more detailed risk assessment is required to drive the assurance plan. *Quickstart* as well as the awareness and diagnostic tools are aids to perform high-level assessments quickly and efficiently.

Planning and reporting—and scoping to a lesser extent—use most of the COBIT components but usually only as input or reference. On the other hand, detailed planning and scoping, as well as testing, are activities that use fewer of the COBIT components but they tend to use them more intensely. Planning, scoping and testing are also the IT assurance activities that extensively use the material that is at the 'heart' of COBIT: the control objectives.

THE STRONGEST LINKS

Some of the strongest links between COBIT components and IT assurance activities (i.e., where activities can benefit the most from the COBIT materials) are as follows:
- Goals and outcome measures with planning risk-based assurance initiatives
- Risk and value statements with risk assessments and risk substantiation
- Key activities and RACI charts with detailed assurance planning
- Control objectives and practices with testing and evaluating controls
- Maturity models and attributes with process maturity and other high-level assessments

The ITGI publication *IT Control Objectives for Sarbanes-Oxley, 2nd Edition*, also provides strong links between COBIT components and IT assurance activities.

Appendix I—Process Control (PC)

PC1 Process Goals and Objectives
PC2 Process Objectives
PC3 Process Repeatability
PC4 Roles and Responsibilities
PC5 Policy, Plans and Procedures
PC6 Process Performance Improvement

APPENDIX I—PROCESS CONTROL (PC)

PROCESS ASSURANCE STEPS

PC1 Process Goals and Objectives

Control Objective	Value Drivers	Risk Drivers
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.	• Key processes measured efficiently and effectively • Processes in line with business objectives	• Process effectiveness difficult to measure • Business objectives not supported by processes

Test the Control Design

- Ensure that a formal process exists for communicating goals and objectives and that, when updated, such communication is repeated.
- Enquire whether and confirm that process goals and objectives have been defined. Verify that process stakeholders understand these goals.
- Enquire whether and confirm that the IT process goals link back to business goals.
- Confirm through interviews with process stakeholders that the IT process goals are SMARRT.
- Enquire whether and confirm that outputs and associated quality targets are defined for each IT process.
- Walk through the process design with selected process stakeholders and verify whether the process is understood and likely to achieve its objectives.

Test the Outcome of the Control Objective

- Analyse process metrics, targets and performance reports to verify that process goals have SMARRT characteristics and are being measured effectively and efficiently.
- Assess the effectiveness of communicating the process goals and objectives through discussions with personnel at various levels and examination of training materials, memos and other documentation.
- Test the appropriateness of the frequency of communication of goals and objectives.
- Ensure that business goals are supported by IT processes by tracing between the two and identifying unsupported businesses goals.

Document the Impact of Control Weaknesses

- Determine the business impact if process goals and objectives are not linked to the business goals.
- Assess the impact on business processing in the event that process goals are not defined in a SMARRT manner.

PC2 Process Ownership

Control Objective

Assign an owner for each IT process, and clearly define the role 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.

Value Drivers

- Processes operating smoothly and reliably
- Processes interacting with each other effectively
- Process problems and issues identified and resolved
- Processes continually improved

Risk Drivers

- Processes performing unreliably
- Processes not working together effectively
- Gaps in process coverage likely
- Process errors not rectified

Test the Control Design

- Enquire whether and confirm that an owner exists for each IT process.
- Enquire whether and confirm that roles and responsibilities have been defined. Verify that the owners understand and accept these responsibilities.
- Confirm with the process owner and direct supervisor that sufficient authority has been provided to support the role and responsibilities.
- Ensure that processes are in place to assign ownership and accountability for processes and deliverables, including communications.

Test the Outcome of the Control Objective

- Review job descriptions and performance appraisals of the process owner to verify assignment, understanding and acceptance of ownership.
- Review the roles and responsibilities to ensure that they are complete and appropriate.
- Review organisation charts and reporting lines to verify actual authority.
- Verify that processes are interacting with each other effectively.
- Verify that process owners are driving continuous improvement.

Document the Impact of Control Weaknesses

Assess whether the process ownership sufficiently supports achieving business processing services to meet short- and long-range organisational objectives.

PC3 Process Repeatability

Control Objective	Value Drivers	Risk Drivers
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 scalable 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.	• Increased efficiency and effectiveness of recurring activities • Ease of process maintenance • Ability to demonstrate process effectiveness to auditors and regulators • Processes supporting the overall IT organisation goals and enhancing IT value delivery	• Inconsistent process results and likelihood of process errors • High reliance on process specialists • Processes unable to react to problems and new requirements

Test the Control Design

- Enquire whether and confirm that process repeatability is a management objective.
- For important and high-risk processes, review the process steps in detail and ensure that they provide for evidence of management review.
- Confirm which good practices and industry standards were used when defining the IT processes.
- Interview selected process stakeholders and determine adherence to the process.
- Ensure that systems are designed for scalability and flexibility.

Test the Outcome of the Control Objective

- Walk through the process design with the process owner, and verify whether the steps are logical and likely to contribute to the end result.
- Review process documentation to verify the adoption of applicable process standards and degree of customisation.
- Assess the maturity and level of integration of supporting tools used for the process.

Document the Impact of Control Weaknesses

Select data about process results not meeting objectives, and analyse whether the causes relate to process design, ownership, responsibilities or inconsistent application.

PC4 Roles and Responsibilities

Control Objective	Value Drivers	Risk Drivers
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's end deliverables.	• Increased efficiency and effectiveness of recurring activities • Staff members knowing what to do and why, improving morale and job satisfaction	• Uncontrolled, unreliable processes • Processes not supporting the business objectives • Processes not performed as intended • Problems and errors likely to remain unresolved • Process performance likely to be variable and unreliable

Test the Control Design

- Ensure that a process is in place to define and maintain information about the key activities and deliverables. Ensure that the process includes the development of supporting policies, procedures and guidance.
- Ensure that processes are designed to capture accomplishments and include them in employee performance information.

Test the Outcome of the Control Objective

- Confirm through interviews and documentation review that key activities and end deliverables for the process have been identified and recorded.
- Review job descriptions, and verify that roles and responsibilities for key activities and process documentation are recorded and communicated.
- Verify through interviews with owners, management and staff members that accountability for the process and its outputs are assigned, communicated, understood and accepted. Corroborate interview findings through analysis of the resolution to significant process incidents and review of a sample of job performance appraisals.
- Enquire whether and confirm that regular job performance appraisal is performed to assess actual performance against process responsibilities, such as:
  - Executing roles and responsibilities as defined
  - Performing process-related activities in line with goals and objectives
  - Contributing to the quality of the process end deliverables
- Review the resolution to significant process incidents, and review a sample of job performance appraisals to verify whether responsibilities and accountabilities are enforced.
- Review roles and responsibilities with various staff members and ascertain their understanding, whether the allocations are appropriate and whether the reporting relationships are effective.
- Assess whether the roles and responsibilities are designed to support compliance with various activities within the roles.

Document the Impact of Control Weaknesses

Assess whether the roles and responsibilities sufficiently support the achievement of business processing services to meet short- and long-range organisational objectives.

PC5 Policy, Plans and Procedures

Control Objective	Value Drivers	Risk Drivers
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.	• Increased staff awareness of what to do and why • Decreasing number of incidents from policy violations • Policies and associated procedures remaining current and effective	• Processes not aligned with business objectives • Staff members not knowing how to perform critical tasks • Policy violations

Test the Control Design

- Enquire whether and confirm that such rules exist and are communicated, known and applied to how all IT process-related documentation (e.g., policies, plans, procedures, guidelines, instructions, methodologies) that drives an IT process will be developed, documented, reviewed, maintained, approved, stored, used for training and communicated.
- Inspect selected policies, plans and procedures to verify if they were created following the rules and are kept up to date.
- Enquire whether and confirm that responsibilities are defined for developing, maintaining, storing and communicating process-related documentation.
- Enquire whether and confirm that there are documented processes under which policies and procedures are identified, developed, approved, reviewed and maintained to provide consistent guidance.

Test the Outcome of the Control Objective

- Verify that those who perform the activities understand their responsibility.
- Inspect selected documents to verify that they are up to date and understood.
- Review IT process-related documentation and verify if sign-off is done at the appropriate level.
- Review if IT process-related documentation is accessible, correct, understood and up to date.
- Ensure that policies are effectively promulgated through awareness and training.
- Assess, through interviews at all staff levels, whether the policies and procedures are clearly understood and support the business objectives.

Document the Impact of Control Weaknesses

Assess whether all policies, plans and procedures sufficiently support achieving business processing services to meet short- and long-range organisational objectives.

PC6 Process Performance Improvement

Control Objective

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 the performance drivers that enable the achievement of process goals. Define how the data are to be obtained. Compare actual measurement to the target and take action upon deviations, where necessary. Align metrics, targets and methods with IT's overall performance monitoring approach.

Value Drivers

- Process costs optimised
- Processes nimble and responsive to business needs

Risk Drivers

- Process outcomes and deliverables not in line with overall IT and business objectives
- Processes too costly
- Processes slow to react to business needs

Test the Control Design

- Enquire whether and confirm that a process is in place to establish key metrics designed to provide a high level of insight into the operations with limited effort.
- Verify that the design of the metrics enables measurement of achievement of the process goals, resource utilisation, output quality and throughput time to support improvement of the process performance and outcome.
- Enquire whether and confirm that relationships between outcome and performance metrics have been defined and integrated into the enterprise's performance management system (e.g., balanced scorecard) where appropriate.
- Enquire whether and confirm that procedures have been designed to identify specific targets for process goals and performance drivers. The procedures should define how the data will be obtained, including mechanisms to facilitate process measurement (e.g., automated and integrated tools, templates).
- Enquire whether and confirm that processes exist to obtain and compare actual results to established internal and external benchmarks and goals. Verify that for key processes, management compares process performance and process outcomes against internal and external benchmarks and considers the result of the analysis for process improvement.

Test the Outcome of the Control Objective

- Enquire whether and confirm that appropriate metrics are defined to assess process performance and achievement of the process goals.
- Analyse some of the key metrics and corroborate, via other means, whether they provide sufficient insight into goals.
- Enquire whether and confirm that targets have been defined for process goals and performance drivers. Review targets and assess whether they align to the goals and enable efficient and appropriate identification of corrective action.
- Review the procedures for collecting data and measurement to ascertain the effectiveness and efficiency of monitoring.
- Interview process owners and stakeholders to assess the appropriateness of the measurement method and mechanisms.
- For significant goals of important processes, reperform data collection and measurement of targets.
- Inspect a sample of process metrics to assess the appropriateness of relationships between metrics (i.e., whether a performance metric provides insight into the likely achievement of the process outcome).
- Obtain and review major deviations against targets and confirm that action was taken. Inspect the list of actions taken as a result of measurement, and verify whether they have led to actual improvements.
- Enquire if internal and external benchmarks are used and, if so, assess their relevance and identify if appropriate action is taken on significant deviations against the benchmarks.

Document the Impact of Control Weaknesses

Determine the business impact if a set of key metrics is not available to measure the achievement of the process goals, resource utilisation, output quality and throughput time to support improvement of the process performance and outcome.

APPENDIX II—PLAN AND ORGANISE (PO)

P01 Define a Strategic IT Plan
P02 Define the Information Architecture
P03 Determine Technological Direction
P04 Define the IT Processes, Organisation and Relationships
P05 Manage the IT Investment
P06 Communicate Management Aims and Direction
P07 Manage IT Human Resources
P08 Manage Quality
P09 Assess and Manage IT Risks
P010 Manage Projects

APPENDIX II—PLAN AND ORGANISE (PO)

PROCESS ASSURANCE STEPS

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 should improve key stakeholders' understanding of IT opportunities and limitations, assess current performance and clarify 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 establishes concise objectives, plans and tasks understood and accepted by both business and IT.

Control Objective	Value Drivers	Risk Drivers
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 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.	• IT investments' benefit transparent and effective to the enterprise • An effective decision-making process to ensure that investments in IT deliver tangible business benefit • IT investments in line with the business objectives • Shared understanding regarding cost, risk and benefits of IT-enabled business initiatives • Direct relationship between business goals and use of resources for IT	• Ineffective decision making leading to investments in IT that have insufficient return or a negative impact on the organisation • IT not aligned with the business • IT value management lacking the support and commitment of senior management • Undefined or confusing accountability and responsibility • Costs, benefits and risks of IT-enabled business initiatives unclear or misunderstood • IT not compliant with governance requirements, potentially impacting management's and the board's public responsibility

Test the Control Design

- Enquire whether and confirm that the process for preparing a business case exists (e.g., the process will guide entry/exit criteria for business case development, the review process, measurements, the change management process for the business case).
- Enquire whether and confirm that the monitoring process for the business case is based upon established benchmarks, such as those in organisational SLAs or industry and technical standards.
- Enquire whether and confirm that the successes and failures of IT investment programmes are reviewed and the business case analysis process is enhanced as required (e.g., historical data should be analysed, and improvements, lessons learned and best practices should be referenced).

PO1 Define a Strategic IT Plan (cont.)

Control Objective	Value Drivers	Risk Drivers
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.	• IT aligned with the organisation's mission and goals • IT enabling the achievement of the strategic business objectives • Optimised return on IT investment • Opportunities for innovation identified and exploited	• IT seen as a cost factor • The enterprise's mission not being supported by its IT • IT management decisions not following the business direction • Lack of common understanding of business and IT priorities, leading to conflicts about allocation of resources and priorities • Missed opportunities to exploit new IT capabilities

Test the Control Design

- Confirm that the process for communicating business opportunities with IT management is reviewed and the importance of the process is communicated to the business and IT. Consider the update frequency of those processes.
- Enquire whether and confirm through interviews with members of IT management that they helped define enterprise goals. Ask them about their accountability for achieving enterprise goals, determine if they undertook what-if analyses and confirm their commitment to the goals.
- Enquire with business management and IT management to identify business processes that are dependent on IT. Consider whether the business and IT share the same view of systems, including their criticality, usage and reporting.

PO1 Define a Strategic IT Plan (cont.)

Control Objective	Value Drivers	Risk Drivers
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.	• IT plans contributing transparently to the organisation's mission and goals • Clarity of costs, benefits and risks of IT's current performance • Technological opportunities identified and capabilities leveraged • IT capabilities known and operationalised effectively and efficiently to deliver the required solutions and services	• IT capabilities not contributing to the organisation's mission and goals • Investment decisions taken too late • Opportunities and capabilities not leveraged • Ineffective use of existing resources • Inability to identify baselines for current, and requirements for future, system capability and performance

Test the Control Design

- Confirm that appropriate criteria, standards and performance indicators have been established and used to assess and report performance to management and key stakeholders. An action plan for variations and a deviation process should exist.
- Review the performance indicators established for key systems and processes (e.g., strengths and weaknesses, functionality, degree of business automation, stability, complexity, development requirements, technology alignment and direction, support and maintenance requirements, costs, external parties' input).
- Confirm that reviews exist with regard to the achievement of agreed-upon targets defined within the previous tactical IT plan.
- Confirm that a comparison against well-understood and reliable industry, technology or other relevant benchmarks is performed to help assess existing systems and capabilities.

PO1 Define a Strategic IT Plan (cont.)

Control Objective	Value Drivers	Risk Drivers
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.	• Strategic IT plans consistent with business objectives • Strategic objectives and associated accountabilities clear and understood by all • IT strategic options identified and structured, and integrated with the business plans • Reduced likelihood of unnecessary IT initiatives • Strategic IT plans complete and usable	• Business requirements not understood or addressed by IT management • No regular and formal consultation between IT management and business and senior management • IT plans not aligned with business needs • Unnecessary IT initiatives and investments • IT plans inconsistent with the organisation's expectations or requirements • IT not focused on the right priorities

Test the Control Design

- Enquire whether and confirm that a process was followed to document IT's goals and objectives necessary to perform its tasks. They should be defined, documented and communicated, including the:
  - Achievement of the benefits and management of the risks of the IT capabilities
  - Establishment of the current and future performance required to respond to business expectations
  - Provision of information on transparency and how IT delivers value to the business
- Enquire whether and confirm that there is a time frame for the development and execution of the strategic and tactical plans. This time frame should include the interrelationships and dependencies of the execution of the tactical plans. The time frame could vary based on scope, funding and prioritisation.
- Enquire whether and confirm that a process to capture outcome measures, represented by metrics (what) and targets (how much), of IT objectives exists and that the measures relate to business-identified benefits and the strategy's direction.
- Confirm and review the policies and procedures supporting the structured planning approach to determine if they effectively support the process for creating an IT strategic plan.

PO1 Define a Strategic IT Plan (cont.)

Control Objective	Value Drivers	Risk Drivers
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.	• Long-range strategic IT plans capable of being operationalised by short-range tactical IT plans • Effective IT resource allocation • IT plans capable of being continuously monitored and evaluated • Day-to-day performance and resource usage capable of being monitored against strategic targets • Focus provided for IT department and staff	• IT long-range plans not achieved • Available IT resources not leveraged for business benefits • Deviations in IT plans not identified • IT's priorities misunderstood and subject to change • Information to monitor IT's performance not available

Test the Control Design

- Enquire whether and confirm that tactical IT plans exist and that they have been based on the IT strategic plan.
- Confirm that this is done in a structured manner in accordance with established processes and that there is no undue delay between updates of the strategic plan and the subsequent update of the tactical plans.
- Validate that the contents of the IT tactical plan are adequate and that it contains proper project definitions, planning information, deliverables and quantified estimated benefits.
- Review whether the tactical plan addresses IT-related risk.

Control Objective	Value Drivers	Risk Drivers
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.	• Efficient IT resource management • IT initiatives continuously monitored and evaluated • The right mix of IT initiatives for a positive and risk-adjusted return on investment (ROI) • Performance and resource requirements of IT initiatives monitored against defined targets	• Missed business opportunities due to a too-conservative portfolio • Low ROI due to a too-aggressive portfolio • Available IT resources not leveraged • Deviations in IT plans not identified

Test the Control Design

- Enquire whether and confirm that a process is in place that enables identification and prioritisation (based on business benefits) of IT programmes and projects supporting the IT tactical plan.
- Confirm that this process of portfolio management uses appropriate criteria to define and prioritise the different projects and programmes.
- Verify whether business goals and expected business outcomes are documented and reasonable, and whether sufficient information related to budget and effort is present.
- Confirm that the programme/project outcomes are duly communicated to all stakeholders.

Take the following steps to test the outcome of the control objectives:
- Confirm through interviews with steering committee members and other sources that the steering committee members are appropriately represented by IT and business unit leadership (e.g., awareness of roles, responsibility, decision matrix and their ownership).
- Review the approved steering committee charter and assess for relevance (e.g., roles, responsibility, authority, accountability, scope and objectives are communicated and understood by all members of the committee).
- Inspect business cases to determine that the documentation has appropriate content (e.g., scope, objectives, cost-benefit analysis, high-level road map, measures for success, roles and responsibilities, impact of existing IT investment programmes) and that the business cases were developed and approved in a timely manner. Confirm through interviews whether IT-enabled investment programmes, IT services and IT assets are evaluated against the prioritisation criteria (review the documented prioritisation criteria).
- Confirm through interviews with members of IT management that they are informed of future business directions and goals, long-term and short-terms goals, mission, and values.
- Enquire whether and confirm that enterprisewide goals and objectives are incorporated into IT strategic and tactical planning processes and that the strategic planning process includes all business and support activities.
- Confirm by examining documentation, such as meeting minutes or correspondence, that business and IT are both involved in leveraging current technology to create new business opportunities.
- Confirm that a report on current information systems (including feedback on the system, use of the system improvements of changes done on the system) is maintained on regular basis.
- Review the achievement of agreed-upon targets defined within the previous tactical IT plan (e.g., outcome of the performance evaluation could include, but may not be restricted to, current requirements, current delivery compared with requirements, barriers to achieving requirements, and the steps and costs required to achieve agreed-upon business goals and performance requirements).
- Enquire whether and confirm that the risk and cost implications of the required IT capabilities have been documented in the IT strategic plan.
- Confirm that the outcome measures that relate to business-identified benefits have been signed off on by the stakeholders and that the feedback from stakeholders has been taken into consideration.
- Enquire whether and confirm that the approved IT strategic plan is communicated and that there is a process to determine that the plan is clearly understood.
- Confirm through interviews, meeting minutes, presentations and correspondence that the IT strategic plan has been approved by the IT steering committee and the board. Enquire whether and confirm that a formal approval process was followed.
- Enquire whether and confirm that tactical plans are aligned to strategic plans and regularly updated. Confirm through interviews that tactical plans are used as the basis for identifying and planning the projects, acquiring and scheduling resources, and implementing monitoring techniques.
- Enquire whether and confirm that the content of the tactical plans includes clearly stated project definitions, project time frames and deliverables, the required resources and the business benefits to be monitored, performance indicator goals, mitigation plan, contingency plan, communication protocol, roles, and responsibilities.
- Confirm that the selected portfolio/project has been translated into the required effort, resources, finding, achievement, etc., and is approved by business (e.g., meeting minutes, senior management review records).
- Confirm that the required authority to launch the approved projects within the selected programmes has been obtained (meeting minutes, formal approval process, communication of approved project) from business and IT.
- Confirm that projects that have been delayed or postponed or that have not proceeded are communicated to business owners and involved IT staff members.

Take the following steps to document the impact of the control weaknesses:
- Assess the risks (e.g., threats, potential vulnerabilities, security, internal controls) due to the improper allocation of IT investment.
- Assess the additional cost due to the return on investment (ROI) not being maximised in terms of business goals.
- Assess the risks (e.g., threats, potential vulnerabilities, security, internal controls) due to the IT investments not being properly aligned with the overall business strategy.
- Assess the impact of the business investing in self-contained IT systems to meet its requirements.
- Assess the possibility of business dissatisfaction with IT service delivery.
- Assess the risks (e.g., threats, potential vulnerabilities, security, internal controls) due to the inability to execute IT strategic plans.
- Assess the risks (e.g., threats, potential vulnerabilities, security, internal controls) due to projects being started and then failing or incurring unnecessary expenditure.
- Assess the additional cost due to the implementation of a suboptimal solution.
- Assess the risks (e.g., threats, potential vulnerabilities, security, internal controls) due to business outcomes not being understood and, hence, being less effective.

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 Objective	Value Drivers	Risk Drivers
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.	• Improved decision making based on relevant, reliable and usable information • Improved IT agility and responsiveness to business requirements • Support for business functions through accurate, complete and valid data • Efficient data management and reduced redundancy and duplication • Improved data integrity • Meeting fiduciary requirements regarding compliance reporting, security and privacy of data	• Inadequate information for business functions • Inconsistency between information requirements and application developments • Data inconsistency between the organisation and systems • High effort required or inability to comply with fiduciary obligations (e.g., compliance reporting, security, privacy) • Inefficient planning of IT-enabled investment programmes due to lack of information • Accumulation of data that are not relevant, consistent or usable in an economical manner

Test the Control Design

- Verify whether an enterprise information model exists, based on well-accepted standards, and whether it is known by appropriate business and IT stakeholders.
- Verify whether the model is effectively used and maintained in parallel with the process that translates IT strategy into IT tactical plans and tactical plans into projects.
- Assess whether the model considers flexibility, functionality, cost-effectiveness, security, failure resiliency, compliance, etc.

PO2 Define the Information Architecture (cont.)

Control Objective	Value Drivers	Risk Drivers
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.	• Common understanding of business data across the enterprise • Facilitated sharing of data amongst all applications, systems and entities • Reduced costs for application development and maintenance • Improved data integrity	• Compromised information integrity • Incompatible and inconsistent data • Ineffective application controls

Test the Control Design

- Enquire whether and confirm that data syntax guidelines are maintained.
- Enquire whether and confirm that the data dictionary is defined to identify redundancy and incompatibility of data and that the impact of any modifications to the data dictionary and changes made to the data dictionary are effectively communicated.
- Review various application systems and development projects to verify that the data dictionary is used for data definitions.
- Enquire whether and confirm that senior managers agree upon the process for defining data syntax rules, data validation rules and business rules (e.g., consistency, integrity, quality).
- Inspect the data quality programme's plans, policies and procedures to evaluate its effectiveness.

PO2 Define the Information Architecture (cont.)

Control Objective	Value Drivers	Risk Drivers
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.	• Ensured availability of information that supports decision making • The focus of security investments based on criticality • Defined accountability for information integrity, availability and security • Data access consistently permitted based on defined security levels	• Inappropriate security requirements • Inadequate or excessive investments in security controls • Occurrence of privacy, data confidentiality, integrity and availability incidents • Non-compliance with regulatory or third-party requirements • Inefficient or inconsistent information for decision making

Test the Control Design

- Review the data classification scheme and verify that all significant components are covered and completed, and that the scheme is reasonable in balancing cost vs. risk. This includes data ownership with business owners and definition of appropriate security measures related to classification levels.
- Verify that security classifications have been challenged and confirmed with the business owners at regular intervals.

Control Objective	Value Drivers	Risk Drivers
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.	• Consistency of data integrity across all data stored • Improved data integrity	• Data integrity errors and incidents • Unreliable data on which to base business decisions • Non-compliance with regulatory or third-party requirements • Unreliable external reports

Test the Control Design

- Enquire whether and confirm that integrity and consistency criteria for all information are defined in collaboration with business management.
- Enquire whether and confirm that procedures are implemented to manage and maintain data integrity and consistency throughout the complete data process and life cycle.
- Enquire whether and confirm that a data quality programme is implemented to validate and ensure data integrity and consistency on a regular basis.

Take the following steps to test the outcome of the control objectives:
- Review documentation of the information architecture model to determine whether it addresses all significant applications and their interfaces and relationships.
- Review information architecture documentation to verify that it is consistent with the organisation's strategy and strategic and tactical IT plans.
- Ensure that changes made to the information architecture model reflect those in the IT strategic and tactical plans and that associated costs and risks are identified.
- Enquire whether and confirm that business management and IT understand relevant parts of the information architecture model (e.g., data ownership, accountability, data governance).
- Enquire whether and confirm that the information architecture model is regularly checked for adequacy, flexibility, integrity and security and that it is subject to frequent user reviews (e.g., impact of information system changes).
- Enquire whether and confirm that data administration controls exist, and co-ordinate the definitions and usage of reliable and relevant data consistent with the enterprise information model.
- Review the data dictionary and verify that all significant data elements are described properly as per the defined process.
- Verify defined data syntax rules, data validation rules and business rules as per the defined process.
- Enquire whether and confirm that metadata in data dictionaries are sufficiently detailed to communicate syntax in an integrated manner across applications and that they include data attributes and security levels for each data item.
- Enquire whether and confirm that data dictionary management is implemented, maintained and reviewed periodically to manage the organisation's data dictionary and data syntax rules.
- Verify whether the system covers all relevant data elements by comparing a list of data with actual implementation in the tool.
- Enquire whether and confirm that a data quality programme is implemented to increase data integrity, standardisation, consistency, one-time data entry and storage (e.g., use automated evidence collection when possible to test data integrity, standardisation, consistency, one-time data-entry and storage from sample data, embedded audit modules, data analysis using audit software or other integration tools). Use automated tools (e.g., computer-assisted audit techniques [CAATs]) to verify data integrity.
- Enquire whether and confirm that a data classification scheme is defined and approved (e.g, security levels, access levels and defaults are appropriate).
- Enquire whether and confirm that data classification levels are defined based on organisation needs for information protection and the business impact of unprotected information.
- Verify that business owners review the actual classification of information and are aware of their roles, responsibilities and accountability for data.
- Enquire whether and confirm that components inherit the classification of the original assets.
- Verify that all deviations from the data classification inheritance policy have been approved by the data owner.
- Enquire whether and confirm that information and data (including hard copies of data) are labelled, handled, protected and otherwise secured in a manner consistent with the data classification categories.
- Inspect evidence that the required integrity and consistency criteria for data are defined and implemented (e.g., data stored in databases and data warehouses are consistent).
- Enquire whether and confirm that a data quality programme is implemented to validate and ensure data integrity and consistency on a regular basis.

Take the following steps to document the impact of the control weaknesses:
- Assess the impact of inconsistency amongst IT plans described in strategic planning and the enterprise information architecture model.
- Assess the impact of ineffective interface between business and IT decision making.
- Assess the vulnerability to disclosure of sensitive information.

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.

Control Objective	Value Drivers	Risk Drivers
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.	• Improved leveraging of technology for business opportunities • Improved integration of infrastructure and applications via defined standards for technical direction • Improved use of resources and capabilities • Reduced costs for technological acquisitions through reduced platforms and incrementally managed investments	• Technological acquisitions inconsistent with strategic plans • IT infrastructure inappropriate for organisational requirements • Deviations from the approved technological direction • Increased costs due to unco-ordinated and unstructured acquisition plans

Test the Control Design

- Review the process of strengths, weaknesses, opportunities and threats (SWOT) analysis performance to ensure effectiveness of process (e.g., check for measurements of the process and changes made to the process as a result of improvement).
- Confirm through interviews with the CIO and other members of senior management that an appropriate technological risk appetite has been established based on the business strategy.

PO3 Determine Technological Direction (cont.)

Control Objective

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.

Value Drivers

- Improved interoperability
- Improved economies of scale for investments and support staffing
- A technology plan with good balance in cost, requirements agility and risks
- Sufficient, stable and flexible technological infrastructure to respond to information requirements

Risk Drivers

- Inconsistent system implementations
- Deviations from the approved technological direction
- Increased costs due to unco-ordinated and unstructured acquisition plans
- Organisational failure to maximise the use of emerging technological opportunities to improve business and IT capability

Test the Control Design

- Confirm with key staff members that a technology infrastructure plan based on the IT strategic and tactical plans is created.
- Review the plan to confirm that it includes factors such as consistent integrated technologies, business systems architecture and contingency aspects of infrastructure components, transitional and other costs, complexity, technical risks, future flexibility value, and product/vendor sustainability and directions for acquisition of IT assets.
- Enquire with key staff members and inspect the technology infrastructure plan to confirm that changes in the competitive environment, economies of scale for information systems staffing and investments, and improved interoperability of platforms and applications are identified.

Control Objective

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.

Value Drivers

- Improved awareness of technological opportunities and improved services
- Improved awareness of technical and regulatory risks
- Improved evaluation of technological changes in line with the business plan

Risk Drivers

- Non-compliance with regulatory requirements
- High effort required to achieve compliance because of wrong or late decisions
- Technical incompatibilities or maintenance issues within the IT infrastructure
- Organisational failure to maximise the use of emerging technological opportunities to improve business and IT capability

Test the Control Design

- Determine whether, by whom and how current and future trends and regulations are monitored (e.g., technological developments, competitor activities, infrastructure issues, legal requirements and regulatory environment changes, third-party experts) and whether related risks or related opportunities for value creation are properly assessed.
- Verify whether the result of the monitoring is consistently passed on to the appropriate bodies (e.g., IT steering committee) and to the IT tactical and infrastructure planning processes for action.

PO3 Determine Technological Direction (cont.)

Control Objective	Value Drivers	Risk Drivers
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.	• Increased control over information systems asset acquisitions, changes and disposals • Standardised acquisitions supporting the technological direction, increasing alignment and reducing risks • Scalable information systems reducing replacement costs • Consistency in technology throughout the enterprise, improving efficiency and reducing support, licensing and maintenance costs	• Incompatibilities between technology platforms and applications • Deviations from the approved technological direction • Licensing violations • Increased support, replacement and maintenance costs • Inability to access historical data on unsupported technology

Test the Control Design

- Verify that the corporate technology standards are being approved by the IT architecture board. Assess the effectiveness of the process for communication of technical standards to IT staff members (e.g., project managers, information architects). Interview relevant IT personnel to determine their understanding of technical standards.
- Ascertain from IT management that monitoring and benchmarking processes are put in place to confirm compliance to established technology standards and guidelines.
- Evaluate technical feasibility analysis documentation for selected projects to assess compliance with corporate technology standards.

Control Objective	Value Drivers	Risk Drivers
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*.	• Increased accountability and responsibility for architectural decisions • Increased alignment between business strategy and technical IT direction • Consistent understanding of technology architecture throughout the enterprise	• Incompatibilities between technology platforms and applications • Deviations from the approved technological direction • Uncontrolled acquisition, use and possible proliferation of information systems assets

Test the Control Design

- Review the guidelines, plans, processes and meeting minutes of the architecture board. Verify whether they provide architecture guidelines and related advice in line with the business strategy and established information architecture.
- Verify whether the architecture board has considered regulatory compliance and business continuity in its decisions.
- Verify that mechanisms are in place that ensure detection of non-compliance with the standards and guidelines of the architecture board within the project management process.
- Assess the role of the architecture board in following through on required corrections arising from non-compliance with standards in the project management process.

Take the following steps to test the outcome of the control objectives:
- Review the result of the SWOT analysis to verify that business systems architecture, technological direction, migration strategies and contingency aspects are included in the technological direction and infrastructure plans.
- Review appropriate documents to confirm whether market evolutions, legal and regulatory conditions, and emerging technologies (e.g., technological developments, competitor activities, infrastructure issues, legal requirements and regulatory environment changes, third-party experts) are being monitored (e.g., review the output and results of the monitoring activity and verify the action taken based on the analysis).
- Review the IT strategy and IT technological infrastructure plan to ensure that it is aligned with the latest developments in IT that have the potential to impact the success of the business.
- Confirm with the chief architect that ongoing assessments of current status vs. planned infrastructure are taking place. Review the corrective actions identified and executed, and compare these against the approved technology infrastructure plans.
- Inspect the technology infrastructure plan to confirm that changes in the competitive environment, economies of scale for information systems staffing and investments, and improved interoperability of platforms and applications are identified.
- Enquire whether the technology research budget is used in an effective and efficient manner (e.g., number of improvements based on research, improvement in services).
- Inspect technology guidelines to determine that they appropriately support the technological solutions, accurately represent the organisation's technological direction and provide sufficient direction for a wide range of problems.
- Enquire whether and confirm that an IT architecture board has been established and roles, responsibility and accountability have been formally defined.
- Confirm with members of the IT architecture board that meetings are held frequently (e.g., periodic/event basis).
- Determine that all agreed-upon actions from IT architecture board meetings are appropriately recorded, tracked and implemented.

Take the following steps to document the impact of the control weaknesses:
- Assess the risks (e.g., threats, potential vulnerabilities, security, internal controls) that the organisation may not select appropriate technologies that achieve business goals or create new business opportunities (e.g., market leadership).
- Assess the risks (e.g., threats, potential vulnerabilities, security, internal controls) that the technology plans may not consider changes in the competitive environment.
- Assess the impact of economies of scale for information systems staffing and investments that are not achieved.
- Assess the opportunity cost of not realising opportunities to integrate platforms and applications.
- Assess the opportunity cost that potential business opportunities may not be realised.
- Assess the opportunity cost that technology trends may not be taken into account in the development of the IT technology infrastructure plan.
- Assess the risk of non-compliance to legal and regulatory regulations.

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.

Control Objective	Value Drivers	Risk Drivers
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.	• Consistent approach for the definition of IT processes • Organisation of key activities into logical, interdependent processes • Clear definition of ownership of and responsibility for processes and key activities • Reliable and repeatable execution of key activities • Flexible and responsive IT processes	• Framework not being accepted by the business and IT processes not being related to business requirements • Incomplete framework of IT processes • Conflicts and unclear interdependencies amongst processes • Overlaps between activities • Inflexible IT organisation • Gaps between processes • Duplication of processes

Test the Control Design

- Enquire whether and confirm that:
  - The IT processes required to realise the IT strategic plan have been identified and communicated
  - A framework to enable the definition and follow-up of process goals, measures, controls and maturity has been defined and implemented
  - Relationships and touchpoints (e.g., inputs/outputs, and amongst the IT processes, enterprise portfolio management and business processes) have been defined.

PO4 Define the IT Processes, Organisation and Relationships (cont.)

Control Objective	Value Drivers	Risk Drivers
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.	• Support of the board • Board insight into IT value and risks • Faster decisions on important investments • Clear responsibility and accountability for strategic decisions • IT governance integrated into corporate governance • Well-governed IT function	• Lack of representation of IT on the board agenda • IT-related risks and value unknown at the board level • Decisions on investments and priorities not based on joint (business and IT) priorities • IT governance separate from corporate governance • IT not compliant with governance requirements, potentially impacting management's and the board's public accountability

Test the Control Design

- Enquire whether and confirm that the:
  - Charter, scope, objectives, membership, roles, responsibilities, etc., of the IT strategy committee have been defined in a manner that will ensure compliance with strategic directions of the enterprise
  - IT strategy committee is composed of board and non-board members with appropriate expertise on the organisation's dependency on IT and opportunities provided by IT
- Review agendas, papers and minutes of the IT strategy committee to:
  - Ensure that the committee meets on a regular basis to address strategic issues, including major investment decisions, raised by the board of directors or the organisation
  - Assess that the committee is giving appropriate guidance to the board of directors on IT governance and IT strategic issues

PO4 Define the IT Processes, Organisation and Relationships (cont.)

Control Objective	Value Drivers	Risk Drivers
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	• IT strategy in line with the organisation's strategy • IT-enabled investment programmes in line with the organisation's strategy • Business and IT involvement in the prioritisation process • Business and IT involvement in conflict resolution • Business and IT involvement in monitoring performance	• IT strategy not in line with the organisation's strategy • IT-enabled investment programmes not in support of the organisational goals and objectives • Insufficient support and involvement of IT and senior organisational management in key decision-making processes

Test the Control Design

- Enquire whether and confirm that the charter, scope, objectives, memberships, roles, responsibilities, etc., of the IT steering committee result in appropriate implementation of the IT strategic directions of the enterprise.
- Inspect documents such as meeting minutes and the IT steering committee charter to identify the participants involved in the committee, their respective job functions and the reporting relationship of the committee to executive management (e.g., determine prioritisation of IT-enabled investment programmes, track status of projects, and monitor service levels and service improvements).
- Enquire and confirm with business management to ensure that the business takes an active role in the work of the IT steering committee and management is appropriately consulted.

PO4 Define the IT Processes, Organisation and Relationships (cont.)

Control Objective	Value Drivers	Risk Drivers
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 chief information officer (CIO) should be commensurate with the importance of IT within the enterprise.	• IT resources aligned to the strategic priorities • Effective management of IT supporting the business objectives • Senior management commitment in IT decision making at the appropriate level • Business/IT alignment at the organisational level	• Insufficient commitment from senior organisational management • IT resources not effectively supporting the business • IT not given sufficient strategic importance • IT regarded as separate from the business and *vice versa* • Lack of business direction and communication of business initiatives

Test the Control Design

- Enquire whether and confirm that the IT function is:
  - Headed by a CIO or similar function, of which the authority, responsibility, accountability and reporting line are commensurate with the importance of IT within the enterprise
  - Defined and funded in such a way that individual user groups/departments cannot exert undue influence over the IT function and undermine the priorities agreed upon by the IT strategy committee and IT steering committee
  - Appropriately resourced (e.g., staffing, contingent workers, budget) to enable the implementation and management of appropriate IT solutions and services to support the business and to enable relationships with the business

Control Objective	Value Drivers	Risk Drivers
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.	• Effective and efficient support for the business • Staffing requirements and sourcing strategies that support strategic business goals • Flexible and responsive IT organisational structure • Business/IT alignment at the organisational level	• Insufficient business support • Insufficient staffing requirements • Inappropriate sourcing strategies • Inflexibility of IT to changes in business needs

Test the Control Design

- Enquire whether and confirm that:
  - Periodic reviews are performed over the impact of organisational changes as they affect the overall organisation and the structure of the IT function itself
  - The IT organisation has flexible resource arrangements, such as the use of external contractors and flexible third-party service arrangements, to support changing business needs

PO4 Define the IT Processes, Organisation and Relationships (cont.)

Control Objective	Value Drivers	Risk Drivers
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.	• Effective individual performance • Activities allocated to specific positions • Efficient recruitment of appropriately skilled and experienced IT staff • Effective staff performance	• Non-compliance with regulations • Compromised information • Recruitment of staff not working as intended • Fraudulent system usage • Non-responsive IT organisation

Test the Control Design

- Enquire whether and confirm that:
  - Each IT task has been formalised by reviewing documentation and determining whether IT task descriptions are appropriate and updated as required
  - A role has been assigned to IT personnel with corresponding IT tasks. Assess whether personnel understand the role and tasks that have been assigned, and that the tasks are being performed.
  - Accountabilities and responsibilities have been assigned to roles. Verify by inspection of job descriptions, charters, etc., that each role has the necessary accountabilities and responsibilities to execute the role.
  - IT personnel have been informed of their roles. Assess whether changes are communicated to IT personnel and whether the changes are being implemented.
  - Managers periodically confirm the accuracy of the role descriptions. Review role descriptions to determine whether they accurately reflect the roles of team members.
  - Role descriptions outline key goals and objectives and include SMARRT measures
  - SMARRT measures are used in staff performance evaluations
  - All role descriptions in the organisation include responsibilities regarding information systems, internal control and security
  - Management trains staff members regularly on their roles. Interview staff members to determine whether a knowledge of the role has been communicated and understood.
- To determine whether employees are provided with enterprisewide and departmental policies and procedures, review the:
  - Annual policy acknowledgement
  - HR records indicating whether employees were provided with policy documentation during new hire orientation
  - Employee training records

PO4 Define the IT Processes, Organisation and Relationships (cont.)

Control Objective	Value Drivers	Risk Drivers
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.	• Quality assurance as an integral part of IT's responsibilities • Processes in line with the organisation's quality expectations • Proactive identification of improvements to IT functionality and business processes • Proactive identification of quality issues and business risks	• Reputational damage • Undetected quality-related risks that impact the overall business • Increased costs and time delays due to poor quality control • Quality assurance not applied consistently or effectively • Inconsistencies in quality across the organisation • Reduced business performance

Test the Control Design

- Enquire whether and confirm that the QA function includes:
  - A reporting line such that it can operate with adequate independence and report its findings objectively
  - Monitoring processes to ensure compliance with the organisation's QA-related policies, standards and procedures (e.g., compliance with the organisation's development methodology)
  - Acting as a centre of expertise for the development of QA-related policies (e.g., QA requirements in a systems development life cycle), standards and procedures
  - A process adopted and aligned with QA best practices and standards
  - Staff levels and skills commensurate with the size of the organisation and the QA function's responsibilities. Assess the skills to verify that they include quality assurance, IT, controls, processes and communication.
  - Active support from senior management sponsors
  - A defined and documented process for identifying, escalating and resolving issues identified to the QA process
  - A process to report periodically on its findings and recommendations

PO4 Define the IT Processes, Organisation and Relationships (cont.)

Control Objective	Value Drivers	Risk Drivers
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.	• Improved protection and integrity of information assets • Risk, security and compliance responsibilities embedded at senior management level • Senior management support in risk, security and compliance issues • Security mechanisms as effective and efficient countermeasures for the organisation's threats • Proactive identification and resolution of risk, security and compliance issues	• Improper protection of information assets • Loss of confidential information • Financial losses • Lack of management commitment for organisationwide security • Non-compliance risk • Unclear understanding of the organisation's IT risk appetite

Test the Control Design

- Enquire whether and confirm that:
  - Senior management has established an organisationwide, adequately staffed risk management and information security function with overall accountability for risk management and information security. Verify by interviewing key personnel that the reporting line of the risk management and information security function is such that it can effectively design, implement and, in conjunction with line management, enforce compliance with the organisation's risk management and information security policies, standards and procedures.
  - Roles and responsibilities for the risk management and information security function have been formalised and documented
  - Responsibilities have been allocated to appropriately skilled and experienced staff members and, in the case of information security, under the direction of an information security officer
  - The resource requirements in relation to risk management and information security have been regularly assessed by management to ensure that appropriate resources are provided to meet the needs of the business
  - A process is in place to obtain senior management guidance concerning the risk profile and acceptance of significant residual risks. Verify that it functions properly by examining recent situations.

PO4 Define the IT Processes, Organisation and Relationships (cont.)

Control Objective	Value Drivers	Risk Drivers
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.	• Users controlling their data and systems • Defined accountability for the maintenance of data and system security measures • Effective and timely information management processes • Reduced financial losses caused by theft of assets	• Improperly secured business data • Improper protection of information assets • Requirements for protecting business data not in line with the business requirements • Inadequate security measures for data and systems • Business process owners not taking responsibility for data

Test the Control Design

- Enquire whether and confirm that a policy for data classification and system ownership has been developed and communicated.
- Validate that the policy has been applied to major application systems and enterprise architecture and internal and external data communication.
- Verify that the policy for data classification and system ownership supports the protection of information assets, enables efficient delivery and use of business applications, and facilitates effective security decision making.
- Observe the process to register and maintain system ownership and data classification, and assess whether the process is being consistently applied.

Control Objective	Value Drivers	Risk Drivers
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 key performance indicators.	• Effective and efficient execution of IT's roles and responsibilities • Appropriate controls over IT functions • Prompt identification of resourcing issues • Prompt identification of performance issues	• Organisation's goals and objectives not met • Resourcing and performance issues not identified and resolved • Malfunction of IT and business processes • Inadequate monitoring of controls and objectives • Key roles and responsibilities not exercised

Test the Control Design

- Confirm through interviews that supervisory practices have been established, including guidance and training for performance reviews.
- Review records to assess the frequency and extent of supervisory reviews and staff appraisals.
- Assess whether reviews have a sound set of performance expectations and performance criteria.
- Enquire whether and confirm that findings from supervisory reviews and staff appraisals are properly escalated, communicated and followed up.

PO4 Define the IT Processes, Organisation and Relationships (cont.)

Control Objective	Value Drivers	Risk Drivers
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.	• Effective and efficient functioning of business-critical systems and processes • Proper protection of information assets • Reduced risk of financial loss and reputational damage	• Inappropriate subversion of critical processes • Financial loss and reputational damage • Malicious or unintentional damages • Non-compliance with external requirements for segregation of materially significant systems and business processes

Test the Control Design

- Enquire whether and confirm that standards have been established to enforce and ensure appropriate segregation of duties and that these standards are reviewed and changed as needed.
- Assess whether standards have been implemented in assigning roles and responsibilities.
- Enquire whether and confirm that a process exists to identify critical positions and processes that must be subject to segregation of duties.

Control Objective	Value Drivers	Risk Drivers
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.	• Ability of IT staff to support business needs • Cost control • Appropriate size of the IT department • Appropriate skills in the IT department	• IT staff resources unable to meet business needs • Excessive IT internal and/or external staffing costs • Under- or overresourced IT department • Lack of appropriate skills in the IT department

Test the Control Design

- Enquire whether and confirm that available and required IT skills and competencies are regularly reviewed and their impact on IT staffing is analysed, escalated and acted upon, as needed.
- Review major business and operational changes, and assess whether their impact on skills, competencies and staffing requirements are assessed and followed up.
- Assess the sourcing strategies and verify that they support the skill and competency requirements.

PO4 Define the IT Processes, Organisation and Relationships (cont.)

Control Objective	Value Drivers	Risk Drivers
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.	• Properly trained key IT personnel • Reduced dependency on individual key IT personnel • Knowledge sharing • Continuity of IT services • Critical IT roles reliably supported • Succession planning	• Insufficient skills of key IT personnel • Reliance on single knowledge experts • Inadequate knowledge sharing or succession planning • Critical tasks and roles not performed

Test the Control Design

- Enquire whether and confirm that management has formal procedures for considering the staffing coverage for key processes when approving or being notified of absences.
- Assess whether management reviews its dependency on key staff members and has considered contingency actions such as alternative sourcing, documenting key knowledge, training of other staff members, and transferring responsibilities from key staff members to others.

Control Objective	Value Drivers	Risk Drivers
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.	• Contracted staff supporting the needs of the business • Knowledge sharing and retention within the organisation • Protection of the information assets • Control over the contracted personnel's activities	• Increased dependence on key (contracted) individuals • Gaps between expectations and the capability of contracted personnel • Work performed not aligned with business requirements • No knowledge capture or skills transfer from contracted personnel • Inefficient and ineffective use of contracted staff • Failure of contracted staff to adhere to organisational policies for the protection of information assets • Litigation costs from disagreements over expectations for responsibility and accountability

Test the Control Design

- Inspect the policies and procedures describing when, how and what type of work can be outsourced, and determine whether they are being implemented.
- Inspect the policies and procedures for information security responsibilities of contractors, and assess through enquiry whether they are being followed (e.g., background checks are conducted, physical and logical access control requirements are followed, personal identification is secure, and contractors are advised that management reserves the right to monitor and inspect all usage of IT resources, including e-mail, voice communications, and all programs and data files).
- Review the policies and procedures for selecting a contractor, and assess whether they are being implemented.

PO4 Define the IT Processes, Organisation and Relationships (cont.)

Control Objective	Value Drivers	Risk Drivers
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.	• Efficient identification and resolution of issues • Alignment of goals and approaches with business objectives and methodologies • Positive involvement of stakeholders • Clearly defined ownership and accountability for relationship management	• Extended gaps between the identification and resolution of issues • Inadequate identification of improvements • Gaps between business objectives and IT policies, guidelines and methodologies

Test the Control Design

- Enquire whether and confirm that a process for identifying stakeholders has been defined and that a communcations channel and communication plan have been established for each.
- Verify through interviews with key stakeholders their satisfaction with IT's communications, the effectiveness of IT's communications and the adequacy with which feedback from stakeholders is being dealt.

Take the following steps to test the outcome of the control objectives:

- Review the IT process framework and determine if it supports the IT strategic plan and integrates with the business process, IT processes and enterprise portfolio management.
- Enquire through interviews whether this framework is being communicated, executed and understood by business and IT.
- Enquire whether and confirm that the IT process framework has been integrated with the quality management system and internal control framework.
- Enquire whether and confirm that the scope, membership, responsibilities, etc., of the IT strategy committee are defined, that the committee is composed of board and non-board members, and that each has appropriate expertise.
- Confirm through interviews, meeting minutes and reports to the board of directors that the IT strategy committee reports to the board on governance and IT strategic issues.
- Enquire whether and confirm that senior IT management understands which processes are used to monitor, measure and report on IT function performance.
- Confirm the existence of an IT steering committee with representation from the executive level, key business operations areas, IT and key business support areas.
- Enquire whether and confirm that formal documentation of the role and authority of the IT steering committee includes key sponsorship at the executive level.
- Inspect documents such as meeting minutes and an IT steering committee charter to identify the participants involved in the committee, their respective job functions and the reporting relationship of the committee to executive management.
- Enquire whether and confirm that IT is headed by a CIO or similar function and the reporting line is commensurate with the importance of IT.
- Confirm through interviews and organisational chart reviews that no individual user groups/departments can exert undue influence over the IT function (e.g., reporting relationship of the IT function and its independence from a single business unit or department, and identifying how projects are funded).
- Confirm through interviews and documentation reviews that the IT function is adequately resourced and funded to support the business function (e.g., review the business case, IT strategy and IT tactical plan for resource requirements).
- Enquire whether and confirm that periodic reviews of the IT organisational structure occur, with the aim of ensuring that they reflect business needs.
- Confirm with the head of IT administration that access to external resources is available as needed.
- Confirm through interviews with IT personnel that a role has been assigned to each with corresponding IT tasks (e.g., assess whether personnel understand the role and tasks that have been assigned and the tasks are being performed).
- Enquire whether and confirm that responsibilities have been assigned to roles (e.g., verify that each role has the necessary responsibilities to execute the role).
- Enquire whether and confirm that role descriptions have been created, and delineate authority and responsibilities.
- Enquire whether and confirm that a QA function exists.
- Determine the role of the QA functions (e.g., monitoring processes to ensure compliance with the organisation's QA-related policies, standards and procedures; and acting as a centre of expertise for the development of QA-related policies, standards and procedures).
- Enquire whether and confirm that the QA function is adequately staffed with the appropriate skills.
- Enquire whether and confirm that members of senior management have established risk management and information security functions that are accountable for the respective areas.
- Enquire whether and confirm that the reporting line of the risk management and security function allows it to effectively design, implement and, in conjunction with line management, enforce compliance with the organisation's policies and procedures.
- Enquire whether and confirm that a process is in place to obtain senior management guidance on the acceptable level of risk associated with IT.
- Enquire whether and confirm that roles and responsibilities for the risk management and information security function have been formalised and documented and that responsibilities have been appropriately allocated. Review the documentation and determine whether roles and responsibilities are being fulfiled as outlined.
- Enquire whether and confirm that resource requirements are assessed regularly and are provided as needed. Assess whether the staffing levels are appropriate based on the the results of the resource requirement assessments.
- Confirm through interview and documentation reviews that an inventory of information assets has been created, tracked and maintained.
- Confirm through interviews that supervisors have the required skill set to perform supervisory functions (e.g., tracking of critical tasks, key performance indicators, staff performance appraisals and risk assessment).
- Review the escalation procedure and verify that it has been implemented and is being applied consistently (e.g., issues are recorded, tracked and analysed periodically).
- Enquire whether and confirm during periodic employee reviews that supervisory skills are assessed and required actions are taken to ensure competency.
- Enquire whether and confirm that there is a process to identify conflicting functions.
- Enquire whether and confirm that conflicting functions have been remediated.
- Enquire whether and confirm that procedures address how appropriate segregation is maintained during periods when typical personnel are unavailable.

- Enquire whether segregation of duties is reviewed when job roles and responsibilities are created or updated and whether responsibilities are reassigned where necessary. Determine whether the changes are implemented (e.g., job descriptions clearly delineate authority and responsibility).
- Enquire whether and confirm that compensating controls have been designed and implemented as necessary (e.g., confirm with senior IT management or supervisors on the effectiveness of the compensating controls). Enquire whether and confirm that management periodically reviews staffing requirements in consideration of business/IT environment and strategy, and identifies skills and resource gaps.
- Enquire whether and confirm that management is evaluating sourcing strategies (e.g., business/IT staff co-location, cross-functional training and job rotation) in conjunction with reviewing staffing requirements.
- Enquire whether and confirm that management periodically identifies key processes, skills required to support the processes and key areas that lack job redundancy (e.g., determine the availability of individuals with relevant skills, experience and knowledge to fulfil the critical roles, and inspect documentation that lists the key processes and the designated individuals who support them).
- Enquire whether and confirm that management has considered outsourcing or other support arrangements to provide job redundancy for key processes (e.g., inspect available contracts with third parties to identify the existence of outsourcing provisions).
- Confirm the existence and maintenance of key contact lists and their availability to the appropriate personnel in a timely manner. Confirm that backup personnel are cross-trained.
- Enquire whether and confirm that the policies, procedures, rules and responsibilities are being communicated to the contractor and that the contractor understands that management reserves the right to monitor and inspect all usage of IT resources.
- Enquire whether and confirm that an appropriate individual has responsibility for reviewing the contractor's work and approval of payments.
- Enquire whether and confirm that IT management has defined the key stakeholders and relationships and that roles and responsibilities are communicated with stakeholders (e.g., users, suppliers, security officers, risk managers, regulators).
- Confirm with management that appropriately skilled IT personnel are assigned to manage the relationship (e.g., inspect documents that list the IT contact for each key stakeholder).
- Enquire whether and confirm that feedback is obtained from the key stakeholders (e.g., issues, action items, reports), and assess whether the feedback is being properly used to drive continuous improvement.

Take the following steps to document the impact of the control weaknesses:
- Assess the risk (e.g., threats, potential vulnerabilities, security, internal controls) that a road map to achieve the strategic goals will not be established.
- Assess the risk and additional cost due to IT not being organised optimally to achieve strategic goals.
- Assess the risk (e.g., threats, potential vulnerabilities, security, internal controls) that an IT strategic plan may not be effectively executed.
- Assess the risks (e.g., threats, potential vulnerabilities, security, internal controls) of overreliance on key IT personnel.
- Assess the additional cost of staffing requirements and sourcing strategies not being adjusted to meet expected business objectives and changing circumstances.
- Assess the additional cost of personnel performing unauthorised duties relevant to their respective jobs and positions.
- Assess the risks (e.g., threats, potential vulnerabilities, security, internal controls) that uncontrolled activities of external personnel may compromise the organisation's information assets.

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, the realisation of business benefits and the ROI of IT-enabled investments.

Control Objective	Value Drivers	Risk Drivers
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.	• Insight into the value of IT's contribution to the business, by using standardised investment criteria • IT priorities based on IT value contribution • Clear and agreed-upon budgets • Improved ability to assign priorities based on business cases	• Unclear priorities for IT projects • Inefficient process for financial management • IT budget not reflecting business needs • Weak control over IT budgets • Failure of senior management to approve the IT budgets • Lack of senior management support

Test the Control Design

- Verify that a financial management framework exists, including processes and responsibilities, as a basis for cost, benefit and budget management. Enquire whether and confirm that inputs and outputs of the financial framework have been defined and that management makes regular improvements to the framework based on available financial information.
- Verify that a portfolio of investment programmes, services and assets has been created and maintained. Perform a high-level review of the portfolio to check for completeness and alignment with the strategic and tactical IT plans.
- Enquire whether and confirm that a process exists to communicate relevant cost and benefit aspects of the portfolio to the appropriate budget prioritisation (business cases), cost management and benefit management processes.
- Confirm that the communicated cost and benefit inputs are comparable and consistent.
- Verify that the created IT budget includes projects, assets and services.

PO5 Manage the IT Investment (cont.)

Control Objective	Value Drivers	Risk Drivers
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.	• Priorities that reflect IT goals and requirements of the business and are transparent to all stakeholders • Focused use of resources • Appropriate decision making, balancing cost, continuous improvement, quality and readiness for the future	• Inefficient resource management • Inability to optimise goals and objectives • Confusion, demotivation and loss of agility due to unclear priorities • IT budget not in line with the IT strategy and investment decisions

Test the Control Design

- Enquire whether and confirm that a process and decision-making committee for the prioritisation of IT initiatives and resources has been created. Verify that the committee's responsibilities have been defined in relation to other committees.
- Enquire whether and confirm that all IT initiatives are prioritised within portfolios based on business cases and strategic and tactical plans.
- Review the allocated budgets and cut-offs for consistency and accuracy.
- Verify through inspection of meeting minutes whether the priortisiation decisions have been communicated, and enquire through interviews whether the decisions are reviewed by the budget stakeholder.
- Enquire whether and confirm that a process exists to identify, communicate and resolve significant budget decisions that impact the business case, portfolio or strategic plans.
- Verify that the IT strategy committee and executive committee have ratified changes to the overall IT budget for items that negatively impact the entity's strategic or tactical plans and have suggested actions to resolve these impacts.

PO5 Manage the IT Investment (cont.)

Control Objective	Value Drivers	Risk Drivers
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.	• An effective decision-making process for budget forecasting and allocation • Formally defined spectrum of funding options for IT operations • Identified and classified IT costs • Clear accountability for spending	• Resource conflicts • Inappropriate allocation of financial resources of IT operations • Financial resources not aligned with the organisation's goals • Lack of empowerment, leading to loss of agility • Lack of senior management support for the IT budget

Test the Control Design

- Enquire whether and confirm that a methodology has been implemented to establish, change, approve and communicate a formal IT budget.
- Review the IT budget to verify whether relevant elements (e.g., authorised sources of funding, internal resource costs, third-party costs, capital and operational expenses) are taken into account when creating the budget.
- Enquire whether and confirm that budget contingencies have been identified and a rationale for these contingencies has been approved.
- Verify that the effectiveness of the budgeting process is monitored (cost allocation, service cost allocation and budget variance analysis), and review reports to verify that lessons learned are recorded to make future budgeting more accurate and reliable.
- Enquire whether and confirm that the people involved in the budgeting process (e.g., process, service and programme owners, asset managers) are properly instructed.
- Enquire whether and confirm that there is an approved and consistent budget creation process (e.g., review the budget plans, make decisions about budget allocations, and compile and communicate the overall IT budgets, project cost allocation, service cost allocation and budget variance analysis).

PO5 Manage the IT Investment (cont.)

Control Objective	Value Drivers	Risk Drivers
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.	• Accurate and timely identification of budget variances • Maximised and cost-efficient utilisation of IT resources • Consistently priced service delivery • Transparent IT value contribution • Business understanding of actual cost and benefit of IT	• Misspending of IT investments • Inappropriate service pricing • IT value contribution not transparent

Test the Control Design

- Enquire whether and confirm that a framework has been defined to manage IT-related costs and that IT expenditure categories are comprehensive, appropriate and properly classified.
- Confirm that there is appropriate independence between individuals who capture, analyse and report financial information, and the IT budget holders.
- Review established timescales to determine whether they are aligned with budgeting and accounting requirements and, within IT projects, whether they are structured according to the deliverables timetable.
- Enquire whether and confirm that a method has been defined that collects data to identify specified deviations.
- Verify that systems from which data are collected have been identified.
- Determine whether the information provided by the systems is complete, accurate and consistent.
- Determine how cost-related information is consolidated, how it is presented at various levels in the organisation and to stakeholders, and whether it helps enable the timely identification of required corrective actions.

PO5 Manage the IT Investment (cont.)

Control Objective	Value Drivers	Risk Drivers
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.	• Accurate identification of benefit variances during and after implementation • Accurate information for portfolio decisions, i.e., continue, adjust or retire programmes • Properly priced service delivery • Transparency of IT's contribution to the business • Business understanding of actual cost and benefit of IT	• Misspending of IT investments • Inappropriate service pricing • IT value contribution not transparent • Incorrect perception of IT value contribution

Test the Control Design

- Enquire whether and confirm that the cost management process provides sufficient information to identify, quantify and qualify benefits of delivering IT solutions, providing IT services and managing IT assets.
- Enquire whether and confirm that the allocation of benefits across time allows for meaningful analysis of benefits.
- Review the process for developing metrics for measuring benefits (e.g., obtaining guidance from external experts, industry leaders and comparative benchmarking data).
- Enquire whether and confirm that there is a remediation process for identified benefit deviations.

Take the following steps to test the outcome of the control objectives:
- Enquire whether and confirm that a financial management framework, processes and responsibilities have been defined and maintained to enable fair, transparent, repeatable and comparable estimation of IT costs and benefits for input to the portfolio of IT-enabled business programmes.
- Assess whether the financial management framework provides information to enable effective and efficient IT investment and portfolio decisions, enables estimation of IT costs and benefits, and provides input into the maintenance of IT asset and services portfolios. Determine whether the financial management framework and processes provide sufficient financial information to assist in the development of business cases and facilitate the budget process.
- Verify that investments, IT assets and services are being taken into account in preparing IT budgets.
- Enquire whether and confirm that the current IT budget is tracked against actual costs and that variations are analysed.
- Enquire whether and confirm that information provided by the budgeting process is sufficient to track project costs and assist in the allocation of IT resources.
- Enquire whether and confirm that an effective decision-making process is implemented to prioritise all IT initiatives and allocate budgets accordingly.
- Enquire whether and confirm that a methodology has been implemented to establish, maintain and communicate for change and approval of a formal IT budget.
- Enquire whether and confirm that process, service and programme owners as well as project and asset managers have been instructed in how to capture budget requirements and plan budgets.
- Confirm that there is a budgeting process and that this process is reviewed/improved on a periodic basis.
- Review the cost management framework and verify that it defines all IT-related costs. Verify that the tools used to monitor costs are effective and used properly (i.e., how costs are allocated across budgets and projects, how costs are captured and analysed, and to whom and how they are reported).
- Enquire whether and confirm that the allocation of the budget across time is aligned with IT projects and support activities to allow for meaningful analysis of budget variances.
- Enquire whether and confirm that IT financial management members have been instructed in how to capture, consolidate and report the cost data.
- Enquire whether and confirm that the appropriate level of management reviews the results of cost analysis and approves corrective actions.
- Enquire whether and confirm that responsibility and accountability for achieving benefits as recorded in the business case have been assigned.
- Enquire whether and confirm that the metrics for monitoring IT's and the business's contribution to the business case are collected, reported and analysed at regular intervals.
- Enquire whether and confirm that the identified budget deviations are approved by business and IT management.

Take the following steps to document the impact of the control weaknesses:
- Assess the risks (e.g., threats, potential vulnerabilities, security, internal controls) that:
  - Input into business cases may not take into account current IT asset and service portfolios
  - New investment and maintenance may not influence the future IT budget
  - Cost/benefit aspects of projects may not be communicated to the budget prioritisation, cost management and benefit management processes
  - The allocation of IT resources may not be prioritised as a result of IT's contribution to optimising ROI
  - Ongoing review, refinement and approval of the overall budget and the budgets for individual programmes may not occur
  - Cost deviations may not be identified in a timely manner and the impact of those deviations may not be assessed
  - Opportunities to improve IT's contribution to business solutions may not be considered
  - Not all benefits may be identified in a cost-benefits analysis, resulting in poor prioritisation of projects and projects that could have been considered may be rejected

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.

Control Objective	Value Drivers	Risk Drivers
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.	• Comprehensive IT control environment • Comprehensive set of IT policies • Increased awareness of the organisation's mission • Proper use of applications and IT services	• Miscommunications about organisational mission • Management's philosophy misinterpreted • Actions not aligned with the organisation's business objectives • No transparent IT control environment • Compliance and security issues

Test the Control Design

- Enquire whether and confirm the existence of formal 'tone at the top' communication (e.g., CIO newsletter or intranet page, periodic e-mails, IT vision or guiding principles) designed to define and manage the IT risk and control environment and ensure that it aligns with the organisation's general risk and control environment.
- Determine whether accountability and responsibility have been assigned to individuals for establishing and reinforcing the communications of the control culture.
- Confirm the existence of policies and practices to support the control environment (e.g., acceptable use policies, background checks).
- Inspect for evidence of periodic awareness training on these policies and practices.
- Determine if a process exists to periodically (at least annually) reassess the adequacy of the control environment and risk appetite to ensure that it is aligned with the organisation's changing environment.
- Enquire whether and confirm that HR policies (e.g., background checks on job applicants, awareness training for new hires, signed code of conduct documentation, appropriate consequences for unethical behaviour) support the IT control environment.

PO6 Communicate Management Aims and Direction (cont.)

Control Objective	Value Drivers	Risk Drivers
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.	• Comprehensive IT control and risk framework • IT risk and control awareness and understanding • Reduction of negative business impact when planned and unplanned issues occur	• Sensitive corporate information disclosed • Irregularities not identified • Financial losses • Compliance and security issues

Test the Control Design

- Enquire whether and confirm that a formal IT risk and control framework exists based on acknowledged industry standards/leading practices (e.g., COSO, COSO-ERM, CobiT).
- Assess whether the IT risk and control framework is aligned with the organisation's enterprise risk and control framework and considers the enterprise risk tolerance level.
- Enquire whether and confirm that the IT risk and control framework specifies its scope and purpose and outlines management's expectations of what needs to be controlled.
- Enquire whether and confirm that the structure of the IT risk and control framework is well defined and responsibilities have been clearly stated and assigned to appropriate individuals.
- Enquire whether and confirm that a process is in place to periodically review (preferably annually) the IT risk and control framework to maintain its adequacy and relevancy.

Control Objective	Value Drivers	Risk Drivers
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.	• Appropriate policies and procedures for the organisation • Quality within the organisation • Proper use of applications and IT services • Transparency and understanding of IT costs, benefits, strategy and security levels	• Greater number and impact of security breaches • Unaccepted or unknown policies • Misunderstanding of management's aims and directions • Out-of-date or incomplete policies • Poor organisational security culture • Lack of transparency

Test the Control Design

- Enquire whether and confirm that a hierarchical set of policies, standards and procedures have been created and align with the IT strategy and control environment.
- Enquire whether and confirm that specific policies exist on relevant key topics, such as quality, security, confidentiality, internal controls, ethics and intellectual property rights.
- Enquire whether and confirm that a policy update process has been defined that requires, at minimum, annual reviews.
- Enquire whether and confirm that procedures are in place to track compliance and define consequences of non-compliance.
- Enquire whether and confirm that accountability has been defined and documented for formulating, developing, documenting, ratifying, disseminating and controlling policies to ensure that all elements of the policy management process have been assigned to accountable individuals.

PO6 Communicate Management Aims and Direction (cont.)

Control Objective	Value Drivers	Risk Drivers
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.	• Appropriate protection of the organisation's assets • Decisions aligned with the organisation's business objectives • Efficient management of the organisation's assets • Proper use of IT resources and IT services	• Organisation's policies, standards and procedures unknown or not accepted • Lack of communication of management's aims and directions • Control culture not aligned with management's aims • Policies misunderstood or not accepted • Business risk of policies and procedures not followed

Test the Control Design

- Enquire whether and confirm that a process is in place to translate IT policies and standards into operational procedures.
- Enquire whether and confirm that employment contracts and incentive mechanisms are aligned with policies.
- Enquire whether and confirm that a process is in place to require users to explicitly acknowledge that they received, understand and accept relevant IT policies, standards and procedures. The acknowledgement should be periodically refreshed (e.g., biannually).
- Enquire whether sufficient and skilled resources are available to support policy rollout.

Control Objective	Value Drivers	Risk Drivers
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.	• Clearly communicated management philosophy • Increased awareness of the organisation's mission • Awareness and understanding of risks, security, objectives, etc., within the organisation • Decisions aligned with the organisation's business objectives	• IT objectives not achieved • Poor acceptance or understanding of the organisational policy • Business threats not identified in a timely manner • Lack of understanding of management's aims and directions • Lack of confidence and trust in IT's mission • Breakdown in control and security culture

Test the Control Design

- Enquire whether and confirm that there are management processes to regularly communicate IT objectives and direction.
- Verify with a representative sample of staff members at different levels that IT objectives have been clearly communicated and understood.
- Review past communications and verify that they cover the mission, service objectives, security, internal controls, quality, code of ethics/conduct, policies and procedures, etc.

Take the following steps to test the outcome of the control objectives:

- Assess the frequency, format and content of the communication of the 'tone at the top' messages to determine if it will effectively define and reinforce the control culture, risk appetite, ethical values, code of conduct and requirements of management integrity.
- Inspect for evidence of periodic awareness training on policies and practices that are relevant to support the control environment (e.g., annual code of conduct or ethics training, periodic acknowledgement of acceptable use policies). Assess employees' understanding of IT management's philosophy and risk appetite to determine the extent to which it is aligned with management. Assess through inquiry and observation whether there is a general understanding of key risks and regulatory requirements that affect the IT control environment, or a general understanding of the importance of adhering to IT policies and procedures.
- Determine whether there is an IT risk and control framework that defines the enterprise's overall approach to IT risk and control and that aligns the IT policy and control environment to the enterprise risk and control framework.
- Determine whether the responsibilities associated with implementing and maintaining the IT risk and control framework are being adequately carried out by qualified individuals. Inspect defined risks and controls to determine their adequacy in controlling the confidentiality, integrity and availability of information systems and networks.
- Review IT policies to determine the frequency of updates and whether a re-evaluation has occurred at least annually. Make necessary adjustments and amendments, and determine whether updated IT policies are appropriately communicated across the enterprise.
- Confirm through interviews that resources have been allocated to those who perform appropriate roles and responsibilities for formulating, developing, documenting, ratifying, disseminating and controlling IT policies.
- Verify that sufficient and skilled resources have been allocated to support the rollout process, including monitoring and enforcing compliance. Examine and verify through interviews that operational procedures that support the IT policies and standards have been communicated, understood and accepted by appropriate staff.
- Inspect documentation of acknowledgement and acceptance of IT policies for a sample of employees to determine that it is being consistently administered and periodically refreshed.
- Inspect evidence to ensure that communication takes place to articulate IT objectives and direction and that management support is visible.
- Enquire whether and confirm that the communication process has the necessary resources and skills for effective communication.

Take the following steps to document the impact of the control weaknesses:

- Determine whether lack of appropriate IT policy management has resulted in lack of adequate control over IT resources and lack of achievement of business objectives.
- Determine whether lack of adequate communication, monitoring, and enforcement of IT policies and standards has resulted in a lack of compliance with those standards and the associated non-achievement of business goals.
- Determine whether lack of awareness of IT objectives and direction has resulted in the lack of achievement of business goals.

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 Objective	Value Drivers	Risk Drivers
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.	• IT skills optimised and aligned with organisational goals • Improved recruitment and retention of the right IT skills to support future business requirements	• IT services for business-critical processes not supported adequately • Ineffective IT solutions • Lack of appropriate IT skills due to IT human resources management not being in line with market conditions

Test the Control Design

- Enquire whether and confirm that an IT HR management plan exists that reflects the definition of skill requirements and preferred professional qualifications to meet tactical and strategic IT needs of the organisation. The plan should be updated at least annually and should include specific recruitment and retention action plans to address current and future requirements. It should also include policies for the enforcement of uninterrupted holiday policy procedures, as applicable.
- Enquire whether and confirm that a documented process for the recruitment and retention of IT personnel is in place and reflects the needs identified in the IT HR plan.
- Confirm that HR professionals regularly review and approve the IT recruitment and retention process to ensure alignment with organisational policies.

Control Objective	Value Drivers	Risk Drivers
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.	• Appropriately qualified and experienced staff for specific job responsibilities • Improved personal career development, contribution and job satisfaction • Continuous development of skills in line with business needs	• IT staff not skilled as required for business critical requirements • IT staff dissatisfied with career progression • More incidents and errors with greater impact

Test the Control Design

- Inspect a sample of job descriptions for a complete and appropriate description of required skills, competencies and qualifications.
- Verify that processes exist and are conducted on a regular basis to review and refresh job descriptions.
- Enquire whether and confirm that management has identified skill needs, including appropriate education, cross-training and certification requirements to address specific requirements of the organisation.

PO7 Manage IT Human Resources (cont.)

Control Objective	Value Drivers	Risk Drivers
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.	• Communication of and adherence to organisation policies, practices and ethics • Clear accountability and responsibility for key functions • Improved alignment of staff contribution to business goals	• Incorrect actions and decisions based on unclear direction setting • Increased errors and incidents caused by lack of supervision • Staff dissatisfaction through poor management and oversight

Test the Control Design

- Inspect a sample of role descriptions to ensure inclusion of an adequate definition of responsibilities, competencies, and sensitive security and compliance requirements.
- Inspect a sample of acknowledgements for acceptance of role descriptions and responsibilities for IT personnel.
- Review terms and conditions of employment for existence of non-disclosure, intellectual property rights, responsibility for information security, internal control, applicable laws and requirements. These should align with the organisation's requirements for non-disclosure of confidential information.
- Inspect the sample of job descriptions for high-risk positions to determine whether the span of control and required supervision is appropriate for each role.

Control Objective	Value Drivers	Risk Drivers
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.	• Enhanced personal contribution and performance toward organisational success • Effective and efficient delivery of each employee's role • Support of technical and management development, increasing personnel retention • Increase in employees' value to the enterprise	• Insufficient security awareness, causing errors or incidents • Knowledge gaps regarding products, services and practices • Insufficient skills, leading to service degradation and increased errors and incidents

Test the Control Design

- Walk through the training effectiveness measurement process to confirm that the critical training and awareness requirements are included.
- Inspect training programme content for completeness and appropriateness. Inspect delivery mechanisms to determine whether the information is delivered to all users of IT resources, including consultants, contractors, temporary staff members and, where applicable, customers and suppliers.
- Inspect training programme content to determine if all internal control frameworks and security requirements are included based on the organisation's security policies and internal controls (e.g., impact of non-adherence to security requirements, appropriate use of company resources and facilities, incident handling, employee responsibility for information security).
- Enquire whether and confirm that training materials and programmes have been reviewed regularly for adequacy.
- Inspect the policy for determining training requirements. Confirm that the training requirement's policy ensures that the organisation's critical requirements are reflected in training and awareness programmes.

PO7 Manage IT Human Resources (cont.)

Control Objective	Value Drivers	Risk Drivers
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.	• Adequately supported critical IT activities that continually meet objectives • Contingency in place for non-availability of key personnel • Reduced risk of incidents by internal IT staff	• Increased number and impact of incidents caused by unavailability of essential skills to perform a critical role • Staff dissatisfaction due to lack of succession planning and job advancement opportunities • Inability to perform critical IT activities

Test the Control Design

- Inspect documentation on key role personnel for reliance on single individuals for critical processes within the IT organisation.
- Enquire whether training programmes incorporate techniques to mitigate the risk of overdependence on key resources. Programmes should include cross-training, documentation of key tasks, job rotation, knowledge sharing and succession planning for critical roles within the organisation.

Control Objective	Value Drivers	Risk Drivers
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.	• Recruitment of appropriate personnel • Proactive prevention of information disclosure and confidentiality standards	• Increased risk of threats occurring from within the IT organisation • Disclosure of customer or corporate information and increased exposure of corporate assets

Test the Control Design

- Inspect selection criteria for performance of security clearance background checks.
- Review for appropriate definition of critical roles, for which security clearance checks are required. This should apply to employees, contractors and vendors.
- Enquire whether and confirm that hiring processes include clearance background checks. Inspect hiring documentation for a representative sample of IT staff members to evaluate whether background checks have been completed and evaluated.

PO7 Manage IT Human Resources (cont.)

Control Objective	Value Drivers	Risk Drivers
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.	• Improved individual and collective performance and contribution to organisational goals • Improved staff satisfaction • Improved management performance from staff feedback and review processes • Effective use of IT staff	• Inability to identify inefficient operations • Ineffective training programme • Dissatisfied and disgruntled staff, leading to retention problems and possible incidents • Loss of competent staff members and related corporate knowledge

Test the Control Design

- Inspect a representative sample of employee job performance evaluations to determine whether criteria for goal setting includes SMARRT objectives. These should reflect the core competencies, company values and skills required for each role. Walk through the job performance evaluation process to determine whether policies and procedures for the use and storage of personal information are clear and comply with the applicable legislation.
- Inspect the remuneration/recognition process to determine if it is in line with performance goals and organisational policy.
- Inspect performance improvement plans to determine alignment with organisational policies and consistent application throughout the IT organisation. Performance improvement plans should include specifically defined goals, timelines for completion and an appropriate level of disciplinary action if improvements are not achieved.

Control Objective	Value Drivers	Risk Drivers
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.	• Efficient and effective continuation of business-critical operations • Improved staff retention • A more secure information environment through timely and appropriate restriction of access	• Unauthorised access when employees are terminated • Lack of smooth continuation of business-critical operations

Test the Control Design

- Enquire and inspect whether exit procedures for voluntary termination of employment are documented and contain all required elements, such as necessary knowledge transfer, timely securing of logical and physical access, return of the organisation's assets, and conducting of exit interviews.
- Enquire whether job change procedures are documented and contain all required elements to minimise disruption of business processes. Examples include the need for job mentoring, job hand-over steps and preparatory formal training. Inspect job change procedures to determine if the procedures are consistently followed.
- Acquire through HR a list of terminated/transferred users (for the past six months to one year).

Take the following steps to test the outcome of the control objectives:
- Inspect the IT human resource plan to verify that the IT needs of the organisation are defined. The IT human resource plan should be based on organisational objectives and include strategic initiatives, applicable regulatory requirements and the associated IT skills required.
- Ensure that current and future needs are assessed against currently available skills and that gaps are translated into action plans.
- Inspect the IT HR management plan and determine whether it addresses retention practices within the IT organisation, including the identification of critical and scarce skills, consideration of personal evaluations, compensation and incentives, development plans, and individual training needs.
- Verify that job descriptions are periodically reviewed and that job descriptions include skill set competencies and qualifications of current personnel. Compare the skill sets of current employees to job description requirements. Inspect professional development plans from a sample of employees to determine the adequacy of career planning. Development plans should include encouragement of competency development, opportunities for personal advancement and measures to reduce dependence on key individuals.
- Review job descriptions to ensure that each is current and relevant. Include the employee handbook/third-party agreements to confirm that the obligations of employees and third-party personnel are clearly stated and appropriate for the given role. Inspect for employee acknowledgement of conditions for employment, including responsibility for information security, internal control, regulatory compliance, protection of intellectual property and non-disclosure of confidential information. Observe whether the amount of supervision applied to high-risk roles is appropriate. Review procedures governing the activities of high-risk roles to determine if supervisory approval is required and has been performed for critical decisions.
- Determine whether appropriate benchmarking of human resource management activities has been performed against similar organisations, appropriate international standards or industry best practices on a periodic basis. Confirm that the level of supervision is appropriate for the sensitivity of the position and responsibilities assigned.
- Inspect automation controls to track changes to privilege user permissions.
- Verify that the personnel training process is being delivered to all new users prior to granting access and is redelivered on an annual basis. Inspect the personnel training programme content for completeness and appropriateness (such as education on the organisation's requirements for internal control and ethical conduct).
- Inspect delivery mechanisms to determine if information is delivered to all users of IT resources, including consultants, contractors and temporary staff members. Where applicable, it should include customers and suppliers as well.
- Verify that the personnel training programme includes certification and recertification processes for appropriate roles.
- Enquire whether and confirm that training materials and programmes have been reviewed regularly for adequacy and include impact on all necessary skills.
- Confirm that a process exists to measure the completion and effectiveness of critical employee training and awareness programmes and requirements.
- Review documented strategies for the reduction of dependence on single individuals in critical roles. Verify the inclusion of segregation of duties. Inspect the process to identify roles suitable for rotation, and confirm that rotation is occurring. Enquire of employees to determine whether knowledge sharing is occurring.
- Inspect the compiled performance evaluation information to assess whether it was compiled completely and accurately. Validate that the information is used in an appropriate manner. Enquire of employees whether management provides appropriate feedback regarding performance during, and following, the performance evaluation. Determine that performance is evaluated against the individual's goals and performance criteria established for the position. Determine if the performance evaluation process is applied consistently and is in line with performance goals and organisational policies.
- Inspect exit procedures and processes for evidence of consistent application throughout the organisation.
- Review the appropriateness of access rights (logical and physical access) related to job changes. Determine the effects on segregation of duties and compensating controls if old access permissions are retained during a period of transition.
- Verify that user accounts have been disabled for terminated users and appropriate access has been applied for transferred users.

Take the following steps to document the impact of the control weaknesses:
- Assess the organisation's dependency on key individuals to ensure that loss of capability and historical knowledge is not realised.
- Assess whether appropriate monitoring and supervision exist to ensure adherence to management policies and procedures, code of ethics, professional practices, terms and conditions of employment, internal controls, information security policy and procedures, and compliance with regulatory requirements.
- Assess the level of awareness for security requirements to ensure compliance with regulatory requirements, protection of intellectual property, organisational reputation and strategic position.
- Determine the adequacy of personnel training programmes to ensure the organisation's ability to attract and retain qualified personnel.
- Assess dependence on key individuals and the IT organisation's ability to provide continuous support of business processes in an efficient and effective manner. Determine whether appropriate segregation of duties exist for key roles to ensure that critical controls function as intended.
- Assess the appropriateness of security-checking mechanisms for key employees to ensure that control over threats within the organisation, such as theft, disclosure and compromise of sensitive corporate assets, is appropriately addressed.
- Determine whether a well-defined, timely and consistently applied performance evaluation process exists and results in the efficient and effective use of IT resources.
- Assess the level of appropriateness and consistency applied to job change policies and procedures to ensure that disruptions of business-critical operations and unauthorised access to secure environments and organisational assets do not occur.

PO8 Manage Quality

A quality management system 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.

Control Objective	Value Drivers	Risk Drivers
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.	• Alignment with and achievement of business requirements for IT • Stakeholder satisfaction ensured • Consistent QA environment understood and followed by all staff members • Efficient, effective and standardised operation of IT processes	• Insufficient quality in services and solutions, resulting in faults, rework and increased costs • *Ad hoc* and, therefore, unreliable QA activities • Misalignment with industry good practices and business objectives • Ambiguous responsibility for quality, leading to quality reduction

Test the Control Design

- Enquire whether the QMS was developed with input from IT management, other stakeholders and relevant enterprisewide frameworks.
- Enquire whether findings from each quality review are communicated to IT management and other stakeholders in a timely manner to enable remedial action to be taken.
- Determine whether IT quality plans are aligned with enterprise quality management criteria and policies.

PO8 Manage Quality (cont.)

Control Objective	Value Drivers	Risk Drivers
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.	• Alignment of the QMS to business requirements and policies • Consistency and reliability of the general quality plan • Effective and efficient operation of the QMS • Increased assurance for enterprisewide management that IT standards, policies, processes, practices and risk management are effective and efficient	• Undefined responsibilities within projects and services • Quality failures in key IT processes • Non-compliance with defined standards and procedures • IT policies, standards, processes and practices inconsistent with current good practices • Failure of IT policies, standards, processes and practices to meet enterprise objectives

Test the Control Design

- Review IT standards and frameworks to determine if they are appropriate for the systems, data and information in the environment.
- Inspect the authorisation of deviations to IT standards to validate adherence to or non-compliance with mandated or adopted standards.
- Inspect major milestones in key projects to verify that the QMS has been applied.
- Confirm the process for applying changes in mandated or adopted standards within the organisation.

Control Objective	Value Drivers	Risk Drivers
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.	• Efficient and effective use of technology to enable timely achievement of business objectives • Proper identification, documentation and execution of key acquisition and development activities • Formally defined, standardised and repeatable approach for managing acquisitions and developments	• Inaccurate estimations of project timescales and budgets • Unclear responsibilities within projects • Development and implementation errors, causing delays, rework and increased costs • Interoperability and integration problems • Support and maintenance problems • Unidentified errors occurring in production

Test the Control Design

- Enquire whether development and acquisition standards for changes to existing IT resources are applied (e.g., secure coding practices; 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; unit, regression and integration testing).
- Enquire or inspect whether development and acquisition standards enable an appropriate level of control for changes to existing IT resources.
- Enquire whether development and acquisition guidance is incorporated into IT standards and frameworks.

PO8 Manage Quality (cont.)

Control Objective	Value Drivers	Risk Drivers
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.	• Improved customer satisfaction • Quality management aligned with customer expectations • Clarity of roles and responsibilities	• Gaps between expectations and delivery • Failure to adequately understand customer expectations • Failure to adequately respond to customer disputes and feedback • Inappropriate or ineffective customer dispute resolution processes • Inappropriate priority given to different services provided • Disputes with deliverables and quality defects

Test the Control Design

- Enquire whether customer views on the quality management process are obtained. Review the process to verify that views are obtained periodically.
- Inspect for effectiveness the questionnaires, surveys, feedback forms, interviews, etc., from customers.
- Enquire whether customer views on the quality management process are obtained. Review the process to verify that views are obtained periodically.
- Inspect the outputs from the follow-up process to determine if the feedback is organised and useful for improving the complaint-handling process.
- Inspect the documentation of roles and responsibilities to determine if they allow for effective conflict resolution of customer complaints.
- Enquire whether and confirm that customer interaction aspects are included in training programmes.

Control Objective	Value Drivers	Risk Drivers
PO8.5 Continuous Improvement Maintain and regularly communicate an overall quality plan that promotes continuous improvement.	• Improved quality of services and solutions • Improved efficiency and effectiveness in delivery • Improved staff morale and job satisfaction	• Uncontrolled and ineffective service delivery • Service failures • Development faults

Test the Control Design

- Enquire whether findings from each quality review are communicated to IT management and other stakeholders in a timely manner to enable remedial action to be taken.
- Ensure the staff training programme includes effective continuous improvement methodologies.
- Evaluate whether continuous improvement activities are actively promoted, effectively managed and implemented within the quality standards, policies, practices and procedures.
- Enquire whether and confirm that a quality management plan is defined. Inspect the plan and documentation to validate the appropriateness of the learning and knowledge-sharing process.

PO8 Manage Quality (cont.)

Control Objective	Value Drivers	Risk Drivers
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.	• Staff members aware of quality performance • Consistent reporting • Quality reporting integrated into and facilitating the organisation's QMS • Measurable and tangible value of the QMS • Feedback concerning compliance with and usefulness of the QMS	• Lack of clear and consistent quality objectives • Preventive and corrective actions unidentified • Inconsistent quality reporting • Reports failing to contribute to the enterprise's QMS • Lack of clarified objectives • Inconsistent quality reporting • Failure of the QMS to enhance the organisation's objectives • QMS not taken seriously or complied with by the organisation • Weaknesses and strengths within the QMS not recognised • Non-compliance not identified • Projects at risk to be over time and budget and delivered with poor quality

Test the Control Design

- Review executive-level reporting on quality performance (e.g., dashboard reporting and/or balanced scorecard) to identify trends of strengths and weaknesses.
- Inspect whether the quality metrics incorporate the achievement of business and IT strategy, financial cost, risk ratings and available industry data. Review whether the monitoring process enables corrective and preventive actions to take place.
- Perform a walk-through of the quality management process to verify that it considers relevance, applicability, latest industry data and the value of contribution to continuous improvement programmes within the organisation.

Take the following steps to test the outcome of the control objectives:
- Inspect the QMS to verify that it provides a standard and continuous approach for quality management.
- Verify IT management's approval of the QMS.
- Review the periodic performance reviews to determine whether the review programme includes all necessary elements.
- Inspect the results of the periodic independent performance reviews of the QMS.
- Inspect whether follow-up reviews in quality assurance plans exist where significant findings have arisen, and inspect the follow-up reviews to verify that corrective action has been effective.
- Inspect QMS benchmark results to determine if appropriate industry guidelines, standards and enterprises were included in the comparison.
- Inspect the authorisation of deviations to IT standards to validate adherence to or non-compliance with stakeholder requirements.
- Inspect major milestones to verify that the QMS is in operation.
- Inspect the customer quality standards and metric requirements for completeness (i.e., questionnaires, surveys, feedback forms, interviews).
- Inspect the outputs from the QMS follow-up process to determine if the feedback is organised and useful for improving the complaint-handling process.
- Inspect the documentation of roles and responsibilities to determine if it allows for effective conflict resolution of customer complaints.
- Inspect the training programme to verify the existence of customer care content.
- Walk through the periodic performance reviews to determine whether the review programme includes necessary QMS elements.
- Inspect the results of the periodic independent performance reviews of the QMS.
- Inspect whether the quality metrics incorporate the achievement of business and IT strategy, financial cost, risk ratings, and available industry data.
- Review whether the monitoring process enables corrective and preventive actions to take place.
- Perform a walk-through of the QMS process to verify that it considers relevance, applicability, latest industry data and the value of contribution to the continuous improvement programme within the organisation.
- Determine the reliability of quality assurance activities by assessing alignment with industry best practices and gaps between current procedures and business expectations.

Take the following steps to document the impact of the control weaknesses:
- Determine the level of compliance with organisational IT standards and quality practices to assess deviations that may result in incompatible system architecture, leading to increased costs and the project not meeting goals and objectives.
- Determine if development and acquisition standards include processes for accurate estimation of project timescales and budgets to ensure efficient and effective use of IT and business resources and the attainment of strategic goals and objectives.
- Confirm that quality management processes include mechanisms for conflict resolution and the determination of consistency of understanding regarding customer expectations and product/process capability.
- Assess whether customer requirements align with IT standards.
- Determine whether the continuous improvement policy and procedures enable the organisation's ability to maintain a competitive advantage.
- Assess whether quality measurement processes and reporting mechanisms enable corrective actions to be performed in a timely manner.

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 Objective	Value Drivers	Risk Drivers
PO9.1 IT Risk Management Framework Establish an IT risk management framework that is aligned to the organisation's (enterprise's) risk management framework.	• Consistent approach for IT risk management • Effective management of IT risks • Continuous evaluation of current IT risks and threats to the organisation • Broadened IT risk management approach	• IT risks and business risks managed independently • The impact of an IT risk on the business undetected • Lack of cost control for risk management • Each risk seen as a single threat rather than in an overall context • Ineffective support for risk assessment by senior management

Test the Control Design

- Inspect whether the IT risk management framework aligns with the risk management framework for the organisation (enterprise) and includes business-driven components for strategy, programmes, projects and operations. Review the IT risk classifications to verify that they are based on a common set of characteristics from the enterprise risk management framework. Inspect whether IT risk measurements are standardised and prioritised and whether they include impact, acceptance of residual risk and probabilities aligned with the enterprise risk management framework.
- Verify whether IT risks are considered in the development and review of IT strategic plans.

Control Objective	Value Drivers	Risk Drivers
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.	• Effective and efficient use of resources for management of risks • Alignment of risk management priorities to business needs • A focus on relevant and significant risks • Prioritisation of risks	• Irrelevant risks considered important • Significant risks not given appropriate attention • Inappropriate approach to risk assessment

Test the Control Design

- Enquire whether and confirm that an appropriate risk context has been defined in line with enterprise risk management policies and principles and includes processes, such as systems, project management, application software life cycles, management of IT operations and services. Internal and external risk factors should be included.
- Determine whether the IT risk context is communicated and understood.

PO9 Assess and Manage IT Risks (cont.)

Control Objective	Value Drivers	Risk Drivers
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.	• Consistent approach to risk event identification • Focus on significant risk events	• Irrelevant risk events identified and focused on whilst more important events are missed

Test the Control Design

- Inspect the process used to identify potential events and determine if all IT processes are included in the analysis. The design of the process should cover internal and external events. Identification of potential events may include results of former audits, inspections and identified incidents, using checklists, workshops and process flow analysis. Trace identified impacts to the risk registry to determine if the registry is complete, current and aligned with the enterprise risk management framework terminology.
- Enquire whether appropriate cross-functional teams are involved in the different event and impact identification activities. Review a sample of the risk registry for relevance of threats, significance of vulnerabilities and importance of impact, and analyse the effectiveness of the process to identify, record and judge risks.

Control Objective	Value Drivers	Risk Drivers
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.	• Improved planning and use of IT risk management skills and resources • Organisational credibility of IT risk assessment function teams • Knowledge transfer between risk managers • Creation of IT asset value awareness	• Irrelevant risks considered important • Each risk seen as a single event rather than in an overall context • Inability to explain significant risks to management • Significant risks possibly missed • Loss of IT assets • Confidentiality or integrity breach of IT assets

Test the Control Design

- Walk through the risk management process to determine if inherent and residual risks are defined and documented.
- Enquire whether and confirm that the risk management process assesses identified risks qualitatively and/or quantitatively.
- Inspect project and other documentation to assess the appropriateness of qualitative or quantitative risk assessment.
- Walk through the process to determine if the sources of information used in the analysis are reasonable.
- Inspect the use of statistical analysis and probability determinations to measure the likelihood qualitatively or quantitatively.
- Enquire or inspect whether any correlation between risks is identified. Review any correlation to verify that it exposes significantly different likelihood and impact results arising from such relationship(s).

PO9 Assess and Manage IT Risks (cont.)

Control Objective	Value Drivers	Risk Drivers
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.	• Effective management of risks • Consistent approach for risk mitigation • Cost-effective risk response	• Risk responses not effective • Unidentified residual business risks • Ineffective use of resources to respond to risks • Overreliance on existing poor controls

Test the Control Design

Inspect whether risk assessment results were allocated to a mitigating response to avoid, transfer, reduce, share or accept each risk and align with the mechanisms used to manage risk in the organisation.

Control Objective	Value Drivers	Risk Drivers
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.	• Effective management of risks • Continuous evaluation of current risks and threats for the organisation	• Risk mitigation controls that do not operate as intended • Compensating controls that deviate from the identified risks

Test the Control Design

- Enquire whether accepted risks are formally recognised and recorded in a risk action plan.
- Assess the appropriateness of the elements of the risk management plan.
- Enquire or inspect whether execution, report progress and deviations are monitored.
- Inspect risk responses for appropriate approvals.
- Review actions to verify whether ownership is assigned and documented.
- Inspect whether the risk action plan is effectively maintained and adjusted.

Take the following steps to test the outcome of the control objectives:
- Enquire whether the IT risk management tolerance levels are aligned with enterprise risk tolerance levels. Determine whether organisational risk tolerance is used as input for both business and the IT strategy development.
- Enquire whether a process exists to apply enterprise risk tolerance levels to IT risk management decisions. Consider whether benchmarking of the risk assessment framework against similar organisations, appropriate international standards and industry best practices has been performed.
- Test whether risk-related accountability and responsibilities are understood and accepted. Verify that the right skills and necessary resources are available for risk management.
- Enquire through interviews with key staff members involved whether the control mechanism and its purpose, accountability and responsibilities are understood and applied.
- Inspect whether the activities are effectively integrated into IT management processes.
- Inspect whether the identified impacts are relevant and significant for the enterprise and whether they are either over- or under-estimated. Determine whether cross-functional teams contribute to the event analysis process. Verify through interviews and impact reports whether the members of the event identification work group are properly trained on the enterprise risk management framework. Verify whether interdependencies and probabilities are accurately identified during impact assessment. Review any correlation to verify that it exposes significantly different likelihood and impact results arising from such relationships.
- Inspect the risk management process to determine if the sources of information used in the analysis are reasonable.
- Inspect the use of statistical analysis and probability determinations to measure the risk likelihood qualitatively or quantitatively.
- Walk through the process to determine if inherent and residual risks are defined and documented.
- Inspect the risk action plan to determine if it identifies the priorities, responsibilities, schedules, expected outcome, risk mitigation, costs, benefits, performance measures and review process to be established.
- Inspect risk responses for appropriate approvals. Review actions to verify whether ownership is assigned and documented.
- Inspect whether the risk management plan is effectively maintained/adjusted.
- Inspect and review the action plan results to determine if they are performed consistently with the risk framework guidelines and reflect changes to business objective. Review the plan to verify that it is designed in terms of risk avoidance, reduction and sharing. Inspect whether the risk responses to be included are selected on benefit and cost considerations.

Take the following steps to document the impact of the control weaknesses:
- Assess the IT risk management strategy to determine whether it is aligned with the enterprise risk management strategy and organisational risk appetite. Confirm that the potential for unidentified risks, misapplication of IT resources, non-compliance with regulatory requirements and organisational goals has been addressed.
- Assess the accuracy and completeness of event identification, including undetected risk, inefficient and ineffective cost containment, unmitigated risks, uncontrolled aggregated risk levels, loss of organisational assets, harmed reputation, unmet strategic goals, and non-compliance with regulatory requirements.
- Assess the risk action plan's effectiveness at mitigating risks across the enterprise, and examine the correlation of risk and mitigation.
- Review the result of the risk action plan to evaluate effectiveness and ascertain whether owners are responsive and timely in mitigation activities.
- Review risk mitigation activities applied to high-risk threats to assess the effectiveness of the prioritisation.

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 Objective	Value Drivers	Risk Drivers
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.	• An optimised approach for programme management • A standardised, reliable and efficient approach for programme management across the organisation • Enhanced ability to focus on key projects within the programme	• Inappropriate project prioritisation • Disorganised and ineffective approach to project programmes • Misalignment of project and programme objectives

Test the Control Design

- Review the programme management framework to verify:
  - That the framework is adequately designed to assess the aggregated portfolio of IT projects against programme objectives
  - That the programme specifies required resources, including funding, project managers, project teams, IT resources and business resources, where applicable, and that the programme management team assigns accountability for each project, including achieving the benefits, controlling the costs, managing the risks, and co-ordinating the project activities clearly and unambiguously.
  - Where accountability is assigned, that such accountability was accepted; there is a clear mandate and scope; and the person accountable has sufficient authority and latitude to act, requisite competence, commensurate resources, clear lines of accountability, an understanding of rights and obligations, and relevant performance measures.
- Review plans, policies and procedures to verify that the programme management team:
  - Determines the interdependencies of multiple projects in the programme
  - Develops a schedule for completion that will enable the overall programme schedule to be met
  - Identifies programme stakeholders inside and outside the enterprise
  - Establishes appropriate levels of co-ordination, communication and liaison with programme stakeholders
  - Maintains communication for the duration of the programme with programme stakeholders
- Verify that, on a regular basis, the programme management team:
  - Verifies with business management that the current programme as designed will meet business requirements, and makes adjustments as necessary
  - Reviews progress of individual projects and adjusts the availability of resources, as necessary, to meet schedule milestones
  - Evaluates changes in technology and IT markets to determine if adjustments to the programme should be made to avoid newly occurring risks, takes advantage of newer and more effective technological solutions, or takes advantage of changes in the market that can lower costs

PO10 Manage Projects (cont.)

Control Objective	Value Drivers	Risk Drivers
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.	• Increased likelihood of project success • Reduced cost associated with establishing project management activities and disciplines • Effective communication of project objectives, project management activities and project progress • Consistent approach, tools and processes	• Different project management approaches within the organisation • Lack of compliance with the organisation's reporting structure • Inconsistent tools for project management

Test the Control Design

- Review plans, policies and procedures to verify that the project management framework:
  - Is consistent with, and an integral component of, the organisation's programme management framework
  - Includes a change control process for recording, evaluating, communicating and authorising changes to the project scope
  - Is subject to periodic assessment to ensure its ongoing appropriateness in light of changing conditions
  - Includes guidance on the role and use of an existing programme or project office, or the creation of such a function for a project

PO10 Manage Projects (cont.)

Control Objective

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.

Value Drivers

- Optimised use of resources for project management
- Clear roles and responsibilities ensuring clear accountability and commitment for key decisions and tasks
- Enhanced alignment of project objectives with business objectives
- Timely and nimble ability to react to and deal with project issues

Risk Drivers

- Confusion and uncertainty caused by different project management approaches within the organisation
- Lack of compliance with the organisation's reporting structure
- Failure to respond to project issues with optimal and approved decisions

Test the Control Design

- Review plans, policies and procedures to verify that:
  - Prior to each project's initiation, the programme management team establishes a project management governance structure appropriate to the project's size, complexity and risks (including legal, regulatory and reputational risks). The project management governance structure should assign the responsibility and accountability of the programme sponsor, project manager, and, as necessary, those of a steering committee and a project management office.
  - The programme management team assigns each IT project one or more sponsors with sufficient authority to manage execution of the project within the overall strategic programme. This assignment is made unambiguously, roles and responsibilities are made plain, and the responsibility is accepted by the assignee(s).
- Enquire whether and confirm that effective mechanisms to track the execution of the project (e.g., regular reporting, stage reviews) are put in place. Review plans, policies, procedures and reports to verify that the mechanisms are designed effectively by the programme management team and that they are used to identify and manage deviations in a timely manner.

PO10 Manage Projects (cont.)

Control Objective	Value Drivers	Risk Drivers
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.	• Increased likelihood of the project being driven by, and delivering, business benefits • Common understanding of the project objectives across the business, end users and IT • User commitment and buy-in for the project	• Unclear responsibilities and accountabilities for ensuring cost control and project success • Insufficient stakeholder participation in defining requirements and reviewing deliverables • Reduced understanding and delivery of business benefits

Test the Control Design

- Enquire whether and confirm that:
  - The project management framework provides for commitment and participation by key stakeholders, including management of the affected user department and key end users, in the initiation, definition and authorisation of a project
  - Key stakeholder and end-user participation is sought during project initiation and further refined during the project life cycle
- Review project reporting to verify that ongoing involvement includes project approval, project phase approval, project checkpoint reporting, project board representation, project planning, product testing, user training, user procedures documentation and project communication materials development.
- Interview key stakeholders and end users, and inspect results of post-implementation reviews to verify that involvement was used to improve the quality and acceptance of project deliverables.

Control Objective	Value Drivers	Risk Drivers
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.	• Baseline provided against which the progress and, ultimately, the success of the project can be measured • Accountabilities including those of key business stakeholders assigned and clarified • Effective use of resources for the projects • Preparation of a master project plan facilitated	• Misunderstanding of project objectives and requirements • Failure of projects to meet business and user requirements • Misunderstanding of the impact of this project with other related projects

Test the Control Design

- Review plans, policies and procedures to verify that:
  - The project management framework provides to the stakeholders a clear, written statement defining the objective, scope and business value of every project, before work on the project begins, to create a common understanding of project scope amongst stakeholders
  - Requirements for the project are agreed upon and accepted by key stakeholders and programme and project sponsors within the organisation and IT, including initial consideration of high-level critical success factors and key performance indicators
  - All subsequent changes to the project scope are appropriately documented and approved by stakeholders

PO10 Manage Projects (cont.)

Control Objective	Value Drivers	Risk Drivers
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.	• Consistent project goals in line with the organisation's vision • Prioritised project execution • Conformance of project phases with the project definition • Ability to monitor and communicate the progress of the project	• Lack of alignment of projects to the organisation's vision • Wrong prioritisation of projects • Undetected deviations from the overall project plan • Poor utilisation of resources

Test the Control Design

- Review plans, policies and procedures to verify that the project management framework provides for designated managers and end users of the affected business and IT functions to approve and sign off on the deliverables produced in each project phase (e.g., requirements analysis, design, build, test, go-live) of the systems development life cycle, before work on the next phase begins.
- Enquire whether and confirm that the approval process is based on clearly defined acceptance criteria agreed upon with key stakeholders prior to work commencing on the project phase deliverable and, at a minimum, in advance of the completion of the deliverables for a phase.
- Review plans, policies and procedures to verify that phase initiation and approval includes consideration of actual costs, time and progress for the phase vs. the budgeted values.
- Review plans, policies and procedures to verify that significant variances are assessed against the project's expected benefits, approved by the appropriate programme governance function and reflected in the programme's business case.
- Review plans, policies and procedures to verify that, prior to implementation, the readiness of the project to go live is approved through a formally conducted 'stop/go' assessment based on predetermined critical success factors aimed at determining system quality and the preparedness of the business and support functions to use and maintain the system.

PO10 Manage Projects (cont.)

Control Objective	Value Drivers	Risk Drivers
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.	• Increased probability that project milestones for time, budget or scope are met • Increased management awareness of potential project slippage, and the ability to react in a timely manner • A mechanism for sharing project plan and progress details in a consistent manner within, and external to, the project • Progress of project evidenced and communicated	• Undetected errors in project planning and budgeting • Lack of alignment of projects to the organisation's objectives and to other interdependent projects • Undetected deviations from the project plan

Test the Control Design

- Review plans, policies and procedures to verify that the integrated project plan provides information to permit management to control project progress and that the plan includes a statement of scope, details of project products and deliverables, required resources and responsibilities, clear work breakdown structures and work packages, estimates of resources required, milestones, key dependencies, and identification of a critical path.
- Enquire whether and ensure that the integrated project plan and any dependent plans are updated with the agreement plan owner to reflect the actual progress and material changes from master project plan checkpoints.
- Enquire whether and confirm that the project plan includes a communication plan that addresses changes and status reporting to key stakeholders.

Control Objective	Value Drivers	Risk Drivers
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.	• Skills and resources efficiently and effectively allocated and assigned within the project • Timely detection of resource gaps • Project resource allocation in line with the corporate procurement policy	• Gaps in skills and resources jeopardising critical project tasks • Inefficient use of resources • Contract disputes with outsourced resources

Test the Control Design

- Enquire whether and confirm that resource needs are identified for the project and appropriate roles and responsibilities are clearly mapped out, with escalation and decision-making authorities agreed to and understood.
- Enquire whether and confirm that roles are identified and staffed with appropriate personnel.
- Enquire whether and confirm that an experienced project management resource and team leader are utilised, with skills appropriate to the size, complexity and risk of the project being undertaken.
- Inspect plans, policies and procedures to verify that the roles and responsibilities of other interested parties are considered and clearly defined (e.g., interested parties include, but are not limited to, internal audit, compliance, finance, legal, procurement and HR).
- Enquire whether and confirm that responsibility for procurement and management of third-party project and system support relationships is clearly defined.

PO10 Manage Projects (cont.)

Control Objective	Value Drivers	Risk Drivers
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.	• Early identification of potential showstoppers when considering project feasibility and approval • Management able to identify and plan for contingencies and countermeasures to reduce risk impact • Clearly identifiable risk and issue owners • Mitigating actions monitored • Consistent and efficient approach for risk management within projects aligned to the organisation's risk management framework	• Undetected project risks • Lack of mitigating actions for identified risks • Undetected project showstoppers

Test the Control Design

- Enquire whether and confirm that a formal project risk management framework has been established.
- Review plans, policies and procedures to verify that responsibility for executing the organisation's project risk management framework within a project is clearly assigned to an appropriately skilled individual.
- Review plans, policies and procedures to verify that this role may be performed by the project manager or delegated by the project manager to another member of the project team.
- Enquire whether and confirm that a project risk assessment was performed to identified project risks and issues.
- Enquire whether and confirm that project risks are reassessed periodically, including at entry into each major project phase and as part of major change request assessments.
- Inspect documentation to verify that risk and issue owners are identified; actions for risk avoidance, acceptance or mitigation (i.e., contingency plan) are identified for these risks; corrective actions are assigned to owners; cost implications are considered; and actions are managed to agreed-upon action due dates.
- Enquire whether and confirm that a project risk log and a project issues log are maintained and reviewed regularly.

PO10 Manage Projects (cont.)

Control Objective	Value Drivers	Risk Drivers
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.	• Alignment of the project quality plan with the corporate quality framework • Increased likelihood of the implemented system or system modification meeting business and user requirements • A consistent level of quality assurance activity across the project, including third parties	• Project deliverables failing to meet business and user requirements • Gaps in expected and delivered quality within the projects • Inefficient and fragmented approach to quality assurance • Implemented system or changes adversely impact existing systems and infrastructure

Test the Control Design

- Review plans, policies and procedures to verify that the quality plan clearly identifies ownership/responsibilities, processes and metrics to provide quality assurance of the project deliverables that make up the project quality system.
- Review plans, policies and procedures to verify that the quality plan outlines the requirements, where appropriate, for independent validation and verification of the business and technical solution.

Control Objective	Value Drivers	Risk Drivers
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.	• Clear priorities for managing resource conflicts • Ability to track the project scope • Decisions relating to changes in the project made safely and efficiently	• Lack of control over project scope, cost and schedule • Lost business focus • Inability to manage resources

Test the Control Design

- Enquire whether and confirm that a change control process exists to manage, assess, justify and approve project changes. Assess the appropriateness of the change request as part of the process.
- Inspect a sample of project change requests to determine whether they are initiated by designated individuals and contain a complete description of the change, associated risks and expected benefits.
- Enquire whether and confirm that the programme and project plan and documentation are updated for approved changes.

PO10 Manage Projects (cont.)

Control Objective

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.

Value Drivers

- External requirements for assurance (e.g., external audit) satisfied in a timely and cost-effective manner
- External accreditation of systems or systems modifications facilitated
- Key stakeholders' increased confidence that the project is under control and on track to realise business benefits

Risk Drivers

- Untrustworthy assurance activities
- Ineffective and/or inefficient assurance activities
- Accreditation and implementation delays

Test the Control Design

- Enquire whether and confirm that project management standards and procedures include steps to consider compliance requirements (e.g., testing internal controls and security requirements).
- Inspect project management standards and procedures to determine if they include steps to consider compliance requirements. Inspect requirements documentation for projects impacting compliance to determine that appropriate compliance stakeholders are involved and requirements are approved.
- Inspect documentation for projects that include systems with accreditation, assurance or validation requirements to determine if appropriate subject matter specialists were involved in requirements testing and approving results.

Control Objective

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.

Value Drivers

- Improved customer satisfaction and focus
- Strong customer bias in the culture of the IT organisation for all IT projects
- Deviations to the plan promptly identified
- Positive results communicated and built upon to boost stakeholder confidence and commitment

Risk Drivers

- Ineffective reporting on project progress and unidentified issues
- Lack of control over project progress
- Loss of focus on customer expectations and business needs

Test the Control Design

- Enquire whether and confirm that the IT programme, project governance and management frameworks consist of the presence of key IT project performance criteria, including scope, schedule, quality, cost and level of risk.
- Review baseline project plans to determine if the IT programme management team recommends, implements and monitors remedial action when required. The plans should be in line with the programme and project governance framework.

PO10 Manage Projects (cont.)

Control Objective	Value Drivers	Risk Drivers
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.	• Increased likelihood that the project will realise expected and agreed-upon business benefits • Improvements identified in project management and system development for future projects • Increased focus on executing remaining actions for delivery of promised benefits	• Undetected project management weaknesses • Missed opportunities from lessons learned

Test the Control Design

- Enquire whether and confirm that IT policies and procedures include key steps for project closure, including an effective post-implementation review.
- Inspect documentation of a sample of post-implementation reviews to determine if the reviews are effectively planned and executed.
- Walk through the process used to identify, communicate and track any uncompleted activities required to achieve project programme benefits. Inspect post-implementation documentation to determine if uncompleted activities are identified, communicated and resolved.
- Walk through the process used to collect lessons learned to determine if the process is effective in improving future projects. Assess customer involvement in the review and analysis process.

Take the following steps to test the outcome of the control objectives:

- Inspect documentation of the programme management framework to verify that the programme adequately assesses the aggregated portfolio of IT projects against programme objectives. The programme should specify required resources, including funding, project managers, project teams, IT resources and business resources, where applicable.
- Inspect documentation and trace activities through the process to verify that the programme management team also specifies required resources, including funding, project managers, project teams, IT resources and business resources, where applicable.
- Inspect documentation and trace activities through the process to verify that the programme management team effectively assigns accountability for each project and that, where accountability is assigned, such accountability is accepted and the person accountable has sufficient authority and latitude to act, requisite competence, commensurate resource, clear lines of accountability, an understanding of rights and obligations, and relevant performance measures.
- Inspect schedules and other documentation to determine whether the programme management team effectively discovered the interdependencies of multiple projects in the programme and developed a schedule for their completion that enables the overall programme schedule to be met.
- Inspect communications and other documents to determine that the programme management team effectively determines programme stakeholders inside and outside the enterprise; establishes appropriate levels of co-ordination, communication and liaison with these parties; and maintains communication with them for the duration of the programme.
- Inspect periodic assessments and other documents to verify that the project management framework is used effectively as an integral component of, and is consistent with, the organisation's programme management approach, and that it is appropriate in light of changing conditions.
- Inspect major milestones to validate that appropriate sign-offs have been achieved before proceeding to the next phase (e.g., a review committee consisting of sponsors and end users to ensure that scope and requirements are appropriate).
- Inspect documentation to verify that the programme management team effectively assigns each IT project one or more sponsors with sufficient authority to manage execution of the project within the overall strategic programme, the assignment is made unambiguously, roles and responsibilities are made clear, and the responsibility is accepted by the assignee(s).
- Inspect documentation such as meeting minutes and sign-off documentation to verify that the project management team effectively provides for commitment and participation by key stakeholders, including management of the affected user department and key users, in the initiation, definition and authorisation of a project.
- Inspect documents such as meeting minutes and sign-off documentation and trace activities through the process to verify that the ongoing key stakeholder commitment and participation for the remainder of the project life cycle is effectively outlined during the project initiation and an effective refining process is used further during the process.
- Verify that the project/programme communication plan is effectively maintained throughout the project.
- Sample change requests to verify that stakeholders provided appropriate sign-off.
- Inspect plans, policies and procedures to verify that the project management framework is designed effectively to provide for designated managers and end users of the affected business and IT functions to approve and sign off on the deliverables produced in each project phase of the system development life cycle, before work on the next phase begins.
- Inspect documentation to verify that the basis of the approval process is effective to clearly define acceptance criteria agreed upon with key stakeholders prior to work commencing on the project phase deliverable and, at a minimum, in advance of the completion of the deliverables for a phase.
- Inspect plans, policies and procedures to verify that phase initiation and approval is designed effectively to consider actual costs, time and progress management, and to assess significant variances against the project's expected benefits.
- Inspect plans, policies and procedures to verify that the appropriate programme governance function is designed effectively to approve assessments of significant variances and that the significant variances are reflected in the programme's business case.
- Physically inspect documentation and search audit trails to verify that the integrated project plan permits management to control project progress.
- Inspect documents to evaluate that the integrated project plan and any dependent plans are kept up to date with the agreement plan holder, to reflect actual progress and material changes from the programme management framework.
- Inspect the project manager organisation chart or RACI chart for completeness.
- Review the project risk assessment and related documentation/meeting minutes to verify that risks (internal and external) are managed and discussed at an appropriate level within the project governance structure throughout the project.
- Determine that the risk management plan is integrated with the overall project plan.
- Inspect assessments and reassessments of risk, change request assessments, and other documents to verify that periodic reassessments are effective and responding to changes in risk over the course of the project.
- Verify that any necessary updates are performed to the risk management plan.
- Inspect documents, search audit trails, and trace transactions through the process to verify that project risk management is being performed effectively, including workarounds for unexpected risks.
- Inspect the project risk log, project issues log and other documents to verify that the project risk log and project issues log are maintained along with corrective actions.
- Inspect documentation to verify that the scope that documents project objectives and major project deliverables is included and a quality process is defined.

Take the following steps to document the impact of the control weaknesses:

- Assess the adequacy of the aggregated portfolio of projects to determine whether it adequately meets business objectives.
- Assess whether resource conflicts exist, project interdependencies are not understood and projects successfully provide ROI.
- Assess the organisation's ability to manage resources effectively and efficiently.
- Assess whether different project management approaches within the organisation utilise resources effectively.
- Assess the organisational reporting structure for appropriate separation of duties.
- Assess project management tools for effective monitoring and reporting.
- Assess compliance with regulatory requirements to determine if resources are utilised effectively to avoid adverse impacts on time, schedule and performance.
- Assess the project sponsor's review and approval of the project scope statement to ensure that objectives are clearly defined and aligned with the IT-enabled investment programme.
- Assess the approved integrated project plan for interdependencies of multiple projects to ensure that project execution and project control exist throughout the life of the project.
- Assess the changes to the integrated project plan for approval and alignment with the programme and project governance framework to identify impacts to costs, schedule and performance.
- Assess whether the project has defined an appropriate governance body to review and provide acceptance to major project phases.
- Assess the organisation's procurement practices to determine whether procurement processes are performed in a timely manner for acquiring and assigning competent staff members and/or contractors to manage the projects cost, schedule and performance.
- Assess the quality management plan to determine consistent levels of quality assurance activity across the project, including third parties.
- Assess whether quality management considerations have been incorporated in a timely manner to ensure cost containment and alignment to the master project plan.
- Assess whether changes are approved or justified and that they meet initial goals and objectives, including any negative impacts to budget, schedules and performance.
- Assess whether assurance tasks provide an appropriate level of system accreditation to provide assurance that internal controls and security features meet the defined requirements.
- Assess whether effective reporting mechanisms exist to monitor project progress.
- Determine management's ability to effectively and efficiently manage project risks.
- Assess project closure for feedback to support future projects of similar type or scope to determine impacts on costs, schedule and performance (e.g., collection of best practices/lessons learned).

Page intentionally left blank

Appendix III—Acquire and Implement (AI)

APPENDIX III—ACQUIRE AND IMPLEMENT (AI)

PROCESS ASSURANCE STEPS

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 Objective	Value Drivers	Risk Drivers
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.	• All significant functional and technical requirements taken into account when considering potential solutions • Complete and accurate set of functional and technical requirements available before development or acquisition begins • Functional and technical requirements defined effectively and efficiently • Selected solution likely to be implemented more quickly and with less rework	• Incorrect solution selected on the basis of an inadequate understanding of requirements • Significant requirements discovered later, causing costly reworking and implementation delays

Test the Control Design

- Confirm through interviews with key staff members that business functional and technical requirements have been defined and a maintenance process has been agreed upon. Inspect documentation of requirements and maintenance processes, and ensure that the design is appropriate to the size, complexity, objectives and risks of the acquisition and has been approved by the relevant owner/sponsor.
- Confirm through interviews with key staff members that all requirements and acceptance criteria have been considered, captured, prioritised and recorded in a way that is understandable to stakeholders and sponsors.
- Confirm through interviews with key staff members that application and infrastructure technical requirements meet the needs of the organisation's information architecture standards and strategic technical direction.
- Review plans, policies and procedures to identify exceptions/deviations from the information architecture standards and strategic technical direction.

AI1 Identify Automated Solutions (cont.)

Control Objective	Value Drivers	Risk Drivers
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.	• Early identification of acquisition risks enabling the reduction or avoidance of potential impact • Increased management awareness of potential risks	• Potentially significant acquisition risks not identified • Management unaware of risks and failure to apply appropriate controls • System security compromised

Test the Control Design

- Confirm through interviews with key staff members, inspection of project documentation, etc., that a holistic approach to the risk analysis of the automated solution is used.
- Confirm through interviews that stakeholders are involved, including representatives from both business and IT.
- Enquire whether and confirm that appropriate risk mitigation mechanisms are considered in the design of the solution and built in from the outset, if justified by the risks the organisation is facing.

Control Objective	Value Drivers	Risk Drivers
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.	• The most effective and efficient solution chosen for the enterprise • Resources available to implement and operate the selected solution • Significant requirements verified before commitment to acquire • Selection decision making based on valid justifications	• Solution failing to meet requirements • Solution failing to perform as expected • Solution failing to integrate with existing infrastructure

Test the Control Design

- Enquire through interviews with key staff members whether a feasibility study process exists that sets out alternative courses of action that will satisfy the business functional and technical requirements (e.g., functionality meets the needs of business and technical requirements).
- Enquire whether and confirm that management and key staff members have determined resources to be used and are aware of go/no-go control checkpoints.
- Confirm with key staff members that the feasibility study includes the potential cost-benefit analysis of each of the identified alternatives and system functionality.

AI1 Identify Automated Solutions (cont.)

Control Objective	Value Drivers	Risk Drivers
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.	• Solution likely to meet business requirements • Solution having business commitment and involvement during implementation • Business having a better understanding of the nature of the solution and the impact it will have on the business processes and organisation	• Solutions failing to meet business requirements • Alternative solutions not identified properly • Business process and organisation aspects of the potential solution inadequately considered

Test the Control Design

- Confirm through interviews with the business sponsor that quality reviews are being performed for business functional and technical requirements and feasibility study reports and that the business sponsor is aware of the original acceptance criteria.
- Evaluate project documentation for a representative sample of projects to ensure that the business sponsor has signed off on the business functional and technical requirements and feasibility reports.

Take the following steps to test the outcome of the control objectives:
- Inspect a selection of correspondence between business sponsors and stakeholders to ensure that key requirements (e.g., definition of user requirements; formulation of alternative courses of action; identification of commercial software packages; performance of technology feasibility, economic feasibility, information architecture and risk analysis studies) have been captured and considered.
- Inspect a selection of requirements documentation to determine whether a proposed new or modified system has been clearly defined, reviewed and approved in writing by the cognisant user before the development, implementation or modification of the project.
- Inspect a selection of application and infrastructure technical requirements documentation to determine if the requirement meets the organisation's information architecture standards and strategic direction (e.g., business continuity planning, disaster recovery planning, security and legal requirements).
- Inspect a selection of risk analysis documentation, and determine whether business and IT risks are identified, examined, assessed and understood by both the business and IT and whether internal control measures and audit trails are identified as part of the risk analysis (e.g., risks on business continuity planning, disaster recovery planning, security and legal requirements).
- Inspect a selection of risk analysis documentation to determine whether risk analysis documentation was signed off on by the key stakeholders, including representatives from the business and IT.
- Inspect a selection of project, audit or other assessment reports and corroborate through interviews with compliance, audit, risk management and security staff members to determine whether a proper balance between detection and prevention controls is considered in the design of the risk response mechanisms.
- Inspect the feasibility study documentation to confirm that technical and economic feasibility met the needs of business and technical requirements.
- Inspect a selection of the feasibility study documentation to confirm that the plan sufficiently accounts for each stage of the acquisition or development life cycle and includes go/no-go control checkpoints.
- Inspect a selection of the technological and economic feasibility study documentation to confirm that identifiable costs and benefits for each of the identified alternatives and system functionalities has been properly supported and included as part of the required technological and economic feasibility study.

Take the following steps to document the impact of the control weaknesses:
- Assess the impact to the time and cost of the project if requirements do not meet user needs.
- Assess the risks (e.g., threats, potential vulnerabilities, security, internal controls) that were not identified due to system development efforts not including robust risk analyses.
- Assess the impact to the time and cost of the project if system development efforts do not comply with policies, laws and regulations.
- Assess the additional cost of the key owner/sponsor not considering alternative courses of action, thereby resulting in a more costly solution.
- Identify deficiencies in the organisation's system development life cycle methodology.
- Identify solutions that do not meet user requirements.
- Identify system development efforts that:
  - Did not consider alternative courses of action, thereby resulting in a more costly solution
  - Did not consider commercial software packages that could have been implemented in less time and at less cost
  - Did not consider the technological feasibility of the alternatives or inappropriately considered the technological feasibility of the chosen solution and, as a result, could not implement the solution as originally designed
  - Made erroneous assumptions in the economic feasibility study and, as a result, chose the wrong course of action
  - Did not consider the information architecture/enterprise data model and, as a result, chose the wrong course of action
  - Did not conduct robust risk analyses and, thus, either did not adequately identify risks (including threats, potential vulnerabilities and impacts) or did not identify appropriate security and internal controls for reducing or eliminating identified risks
- Identify solutions that:
  - Were either overcontrolled or undercontrolled because the cost-effectiveness of control and security was improperly examined
  - Did not have adequate audit trails
  - Did not consider user-friendly design and ergonomic issues, thereby resulting in data input errors that could have been avoided
  - Did not follow the organisation's established procurement approach and, thus, resulted in additional costs being borne by the organisation

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 Objective	Value Drivers	Risk Drivers
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.	• Reduced costs • Consistency between business requirements and high-level design results • Improved time to delivery	• Dependency on knowledge held by key individuals • Undefined development scope • Solutions failing to deliver business requirements • Solutions not aligned with strategic IT plan, information architecture and technology direction • High costs of fragmented solutions

Test the Control Design

- Confirm with key IT staff members that a high-level design specification is defined that translates the business requirements for the software development.
- Obtain and review a sample of a project design specification to determine whether it addresses all the business requirements.
- Confirm with key IT staff members whether the project design approach conforms with the organisation's design standard.
- Review high-level design documentation to determine if the organisation's design standards are being followed.
- Review project documentation, such as the project plan and scoping document, to determine if roles and responsibilities of users in the design process are properly included.
- Corroborate management's views regarding user involvement with users/stakeholders to confirm that users'/stakeholders' expertise and knowledge are considered in the design process of new systems.
- Review supporting documents for unambiguous cross-references, including title and date.
- Confirm with stakeholders (IT and business) that they have approved and signed off on the high-level design and that their inputs have been incorporated into the design (e.g., process owners, information owners, security, user representatives).
- Confirm with stakeholders (IT and business) that the high-level design constitutes a solution that the organisation can deliver, operate and maintain (e.g., IT sponsor, business sponsor).

AI2 Acquire and Maintain Application Software (cont.)

Control Objective	Value Drivers	Risk Drivers
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.	• Reduced costs • Efficient application coding and maintenance • Prioritisation on important features • Avoidance of data redundancy • Application meeting usability requirements	• Processing of invalid transactions • Increasing costs for system redesign • Data in application systems processed incorrectly

Test the Control Design

- Perform code walk-through and examine documentation associated with data inputs and outputs to determine whether proper storage, location and retrieval methods are implemented according to data dictionary standards.
- Examine information architecture and data dictionary documentation to identify deviations from the data dictionary standards in the programme design.
- Enquire of key staff members whether data dictionary standards are being used, and compare actual performance of data inputs/outputs with responses from key staff members.
- Confirm with key staff members that source data collection design is specified that incorporates computed and stored data.
- Perform code walk-through and inspect plans to confirm that data are collected and validated for processing transactions.
- Confirm with key IT staff members that adequate redundancy, failure recovery and backup arrangements are defined and included in the detailed design specification.
- Review the backup plan and procedures to determine that they adequately address the availability requirements of the new system and are cost-effective.
- Enquire of key IT staff members and review relevant project documentation to determine whether file requirements for storage, location and retrieval of data are defined in the detail design specification.
- Review project documentation to determine if best practices, such as availability, control and auditability, security, and network requirements, are considered.
- Enquire of key staff members and inspect relevant project documentation to determine whether processing steps, including transaction types, processing rules including logic transformations or specific calculations are defined and included in the detailed design specification.
- Enquire of key staff members and inspect relevant project documentation to determine whether integration of system (existing or planned subsystems and acquired packaged software) and infrastructure are addressed continuously throughout the process life cycle.
- Confirm with key IT staff members that all identified output data requirements are properly defined.
- Review detail design documentation to determine that pertinent design details, such as different types of recipients, usage, details required, frequency and method of generation, are considered.
- Review detail design requirement documentation to determine if the availability, completeness, integrity and confidentiality of output data as well as the impact of data outputs to other programmes are appropriately addressed.
- Confirm with key staff members that the interface between the user and the system application is defined and included in the detailed design specification.
- Inspect the detailed design specification to confirm that it adequately addresses user interface requirements.
- Enquire about the system design reassessment procedures that address design changes as a result of significant technological and/or logical discrepancies.
- Review documents such as system design analysis reports or system design change requests to confirm that the system design reassessment procedures are followed (e.g., change in system design needs to be approved by business and IT sponsors).
- Review detailed design specification documentation to determine if it was prepared in conformance with organisation- and industry-accepted specification standards and the information architecture.
- Confirm with IT and business stakeholders that a design walk-through takes place before development commences.
- Review the detailed design specification to confirm that a design walk-through is conducted for all stakeholders and that stakeholder sign-off has been initiated before development (e.g., signature and date or e-mail confirmation).

AI2 Acquire and Maintain Application Software (cont.)

Control Objective	Value Drivers	Risk Drivers
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.	• Consistent application controls established • Ensured data integrity • Transaction data history able to be validated and reconstructed, if needed	• Costly compensating controls • Data integrity issues • Gaps between application controls and actual threats and risks • Processing results and data repositories failing to meet compliance requirements

Test the Control Design

- Review the requirements documentation for design of controls to determine that automated application controls are defined based on business process control requirements.
- Review the requirements documentation for design of controls, and identify instances where authorisation, input, processing, output and boundary controls are inadequate.
- Review plans for implementing automated control functions in packaged application software, and determine that business process control requirements are adequately addressed.
- Confirm with business process owners and IT technical design authorities that design specifications for all automated application controls in development or purchased applications are approved.
- Review design specification for all automated application controls in developed or purchased/packaged applications to confirm that they are approved.
- Confirm with project personnel that automated controls have been defined within the application that support general control objectives, such as security, data integrity, audit trails, access control and database integrity controls.
- Perform walk-throughs of application controls in developed and purchased packaged software, trace transactions, and review documentation to ensure that general control objectives (e.g., security, data integrity, audit trails, access control, database integrity controls) are addressed adequately.
- Review project documentation to confirm that design specifications have been assessed against the internal audit, control and risk management standards and objectives.
- Review project documentation to determine if the effects of compensating controls outside the application software realm have been considered.
- Review evidence of high-level review conducted to ensure that automated application and general controls objectives are met (e.g., availability, security, accuracy, completeness, timeliness, authorisation, auditability).

AI2 Acquire and Maintain Application Software (cont.)

Control Objective	Value Drivers	Risk Drivers
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.	• Preventive and detective security controls established as necessary • Ensured data confidentiality, integrity and availability • Maintained system availability for business processing	• Undetected security violations • Costly compensating controls • Gaps between considered security controls and actual threats and risks

Test the Control Design

- Enquire with key staff members to assess knowledge and awareness of how solutions for security and availability in the infrastructure will be integrated with the application.
- Review application acquisition, implementation and testing plans to confirm that application security and availability within the integrated environment have been addressed.
- Enquire whether and confirm that availability design has been approved by technical authorities.
- Inspect documentation sign-off by appropriate stakeholders.
- Interview business sponsors and review walk-through documentation to assess understanding and adequacy of availability design; enquire whether the design is likely to meet the security and availability requirements.

Control Objective	Value Drivers	Risk Drivers
AI2.5 Configuration and Implementation of Acquired Application Software Configure and implement acquired application software to meet business objectives.	• Acquired system configured to meet business-defined requirements • Acquired system compliant with existing architecture	• Loss of business focus • Inability to apply future updates effectively • Reduced system availability and integrity of information

Test the Control Design

- Enquire of business process owners and key staff members to determine whether their input and guidance have been solicited and reflected in the application customisation and configuration. Identify instances where business process owner input has not been solicited.
- Confirm with key staff members whether the application software is customised and configured utilising best practice as advised by vendors and in conformance with internal architecture standards.
- Inspect best practices supplied by vendors, compare with the implementation strategy, and identify inappropriate configuration and customisation.
- Confirm with key staff members that testing procedures are in place that cover verification of acquired application control objectives (e.g., functionality, interoperability with existing applications and infrastructure, systems performance efficiency, integration, capacity and load stress testing, data integrity).
- Inspect unit and integration test documentation and walk-through testing procedures to verify the adequacy of the tests.
- Confirm with key staff members that all user and operation manuals are complete and/or updated where necessary. Trace a sample of customisations to user and operational manuals to confirm documentation updates.

AI2 Acquire and Maintain Application Software (cont.)

Control Objective	Value Drivers	Risk Drivers
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.	• Consistent system availability • Maintained confidentiality, integrity and availability of the processed data • Cost and quality control for developments • Maintained compatibility with technical infrastructure	• Reduced system availability • Compromised confidentiality, integrity and availability of processed data • Lack of cost control for major developments

Test the Control Design

- Confirm with key staff members and inspect relevant documentation to determine that impact assessment of major upgrades has been made to address the specified objective criteria (such as business requirement), the risk involved (such as impact on existing systems and processes or security), cost-benefit justification and other requirements.
- Inspect relevant documentation to identify deviations from normal development and implementation processes.
- Enquire of business sponsors and other affected stakeholders and inspect relevant documentation to determine whether agreement and approval have been obtained for the development and implementation process.

Control Objective	Value Drivers	Risk Drivers
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.	• Ensuring that business, customer and user needs are met • Ability to manage and prioritise resources • Application software creating capabilities for the business • Application meeting usability requirements	• Waste of resources • Lost focus on business requirements • High number of failures • Inability to maintain applications effectively

Test the Control Design

- Confirm with key staff members that all development activity has been established to ensure adherence to development standards and that developed software is based on agreed-upon specifications to meet business, functional and technical requirements.
- Inspect relevant documentation (such as design, code review and walk-throughs) to identify exceptions to specifications and standards.
- Obtain and review assessment documentation of the developed software to confirm adequacy.
- Confirm with key staff members that technical authorities and operations management applications are ready and suitable for migration to the production environment.
- Perform a walk-through of code and identify problems/exceptions.
- Enquire of key staff members to determine compliance with all obligations and requirements.
- Review contractual obligations and licensing requirements relating to third-party developers.

AI2 Acquire and Maintain Application Software (cont.)

Control Objective	Value Drivers	Risk Drivers
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.	• All-embracing test approach • Performed tests reflecting the business processes and requirements • Formally accepted software	• Poor software quality • Retesting of developed software • Tests failing to reflect current business processes • Test data misused and compromising corporate security • Insufficient testing • Breach of compliance requirements

Test the Control Design

- Confirm with key staff members that the software QA plan has been defined, including specification of quality criteria, validation and verification processes, and definition of how quality will be reviewed.
- Review the plan for the criteria listed above, and ensure that QA reviews are conducted independent of the development team.
- Confirm with key staff members that a process for monitoring software quality has been designed and established.
- Review relevant documentation to confirm that the process is based on project requirements, enterprise policies, quality management procedures and acceptance criteria.
- Confirm with key staff members that all quality exceptions are identified and that corrective actions are taken.
- Inspect relevant documentation of QA reviews, results, exceptions and corrections to determine that QA reviews are repeated when necessary.

Control Objective	Value Drivers	Risk Drivers
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.	• Formally defined requirements and clarified business expectations • Compliance with the established change management procedures • An agreed-upon standardised approach for performing changes to the applications in an effective manner	• Unauthorised changes • Changes not applied to the desired systems • Gaps between expectations and requirements

Test the Control Design

- Ensure and confirm that changes to individual requirements are monitored, reviewed and approved by the stakeholders involved.
- Inspect relevant documentation to confirm that all changes and status of changes are recorded in the change management system.
- Identify and report changes that are not tracked.

AI2 Acquire and Maintain Application Software (cont.)

Control Objective	Value Drivers	Risk Drivers
AI2.10 Application Software Maintenance Develop a strategy and plan for the maintenance of software applications.	• Compliance with the established change management procedures • An agreed-upon standardised approach for performing changes to the applications in an effective manner	• Unauthorised changes • Changes not applied to the desired systems • Gaps between expectations and requirements • Reduced system availability

Test the Control Design

- Confirm through interviews with key staff members that an effective and efficient process for application software maintenance activities has been designed to ensure uniform application for all changes and can be performed quickly and effectively.
- Review the process documentation to determine that relevant issues (including release planning and control, resource planning, bug fixing and fault correction, minor enhancements, maintenance of documentation, emergency changes, interdependencies with other applications and infrastructure, upgrade strategies, contractual conditions such as support issues and upgrades, periodic review against business needs, risks, and security requirements) are included.
- Confirm with key staff members that all maintenance changes comply with the formal change management process, including impact on existing applications and infrastructure.
- Inspect relevant documentation to confirm that changes are prioritised to identify those that would be better managed as a formal redevelopment. Identify any deviations from the formal change management process.
- Enquire and confirm with key staff whether changes applied without following the formal change management process have been reviewed and approved.
- Review relevant documentation to identify changes that have not been reviewed and approved.
- Enquire and confirm with key staff whether patterns and volume of maintenance activities are assessed periodically for abnormal trends.
- Inspect relevant analytical results documentation to confirm that all underlying quality or performance problems are appropriately analysed and reported.
- Confirm with key staff members that all maintenance activity has been completed successfully and thoroughly.
- Perform a walk-through of maintenance activities to ensure that all tasks and phases have been addressed, including updating user, systems and operational documentation and interdependencies.
- Identify all changes in contractual conditions, business trends or other upgrades that have not been addressed.

Take the following steps to test the outcome of the control objectives:
- Review project design documentation to confirm that the design is consistent with business plans, strategies, applicable regulations and IT plans.
- Obtain and review a sample of project sign-off documentation to determine whether the projects have gone through QA sign-off and have proceeded with proper approval of the high-level design by IT and business stakeholders (project sponsors).
- Corroborate with IT management and review relevant documentation to determine if the sampled project design specification aligns with the organisation's technological direction and information architecture.
- Review the integration plan and procedures to determine their adequacy.
- Review project documentation to determine if the impact of the new implementation on existing applications and infrastructure has been assessed and appropriate integration approaches have been considered.
- Review end-of-stage documentation to confirm that all development activities have been monitored and that change requests and quality performance and design reviews have been tracked and considered at formal end-of-stage discussions. Also confirm that stakeholders have been fully represented and that the end-of-stage reviews incorporate approval criteria. Inspect problem logs, review documentation and sign-offs to confirm the adequacy of the development activities and identify deviations.
- Review design documentation to confirm that appropriate solutions and approaches to security and availability are designed to adequately meet the defined requirements and build on or extend the existing infrastructure capability.
- Review QA documentation and fault logs to ensure that all significant quality exceptions are identified and corrective actions are taken. Inspect relevant documentation of QA reviews, results, exceptions and corrections to determine that QA reviews are repeated when necessary.
- Obtain and inspect change requests to determine that they are categorised and prioritised. Confirm with key staff members that the impact of all change requests has been assessed.
- Review change control documentation to confirm that changes applied without following the formal change management process have been reviewed and approved and to identify changes that have not been reviewed and approved.
- Inspect the risk analysis documentation, and determine whether business and IT risks are identified, examined, assessed and understood by both the business and IT and that there is evidence that all stakeholders are involved.
- Review the feasibility study documentation to confirm that both technical and economic feasibility have been adequately considered.
- Review quality review documentation, compare with original acceptance criteria, and identify exceptions or deviations from original acceptance criteria.
- Review end-of-stage documentation to confirm that sign-off has been obtained for proposed approaches and/or feedback requiring further feasibility analysis.

Take the following steps to document the impact of the control weaknesses:
- Identify design specifications that do not reflect user requirements.
- Identify data management requirements that are not consistent with the organisation's data dictionary rules.
- Identify new system development or modification projects that contain inadequately defined file, programme, source data selection, input, user-machine interface, processing, and output and/or controllability requirements.
- Identify designs where security and availability were not adequately considered.
- Identify data integrity design deficiencies.
- Identify test plan requirement deficiencies.
- Identify significant technical and/or logical discrepancies that have occurred during system development or maintenance and did not result in reassessment of the system design and, therefore, went uncorrected or resulted in inefficient, ineffective and uneconomical patches to the system.

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 Objective	Value Drivers	Risk Drivers
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.	• Consistent technological planning • Enhanced system security • Balanced hardware and software utilisation • Alignment with strategic IT plan, information architecture and technology direction • Enhanced financial planning	• No acquisition model • Inconsistent technological infrastructure • Technology failing to support business needs • Information security compromises

Test the Control Design

- Confirm with staff members that a plan for the acquisition, implementation and upgrade of the technology infrastructure has been created that satisfies the business functional and technical requirements.
- Review the plan to confirm that it conforms with the organisation's established technology direction and that all key aspects are included.
- Enquire whether and confirm that a process has been defined and implemented to create and maintain an infrastructure acquisition plan that is aligned with the organisation's technology direction.
- Inspect the infrastructure acquisition plan to identify areas where key aspects, such as requirements, risks, transition and migration, have not been addressed.
- Review the financial appraisal for accuracy and overall coverage.

AI3 Acquire and Maintain Technology Infrastructure (cont.)

Control Objective

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.

Value Drivers

- Consistent technological planning
- Enhanced system security
- Balanced hardware and software utilisation
- Data integrity and confidentiality maintained in all system stages

Risk Drivers

- Disruptions in production processing
- Undetected bypassing of access controls
- Unauthorised access to sensitive software
- Business needs not supported by technology

Test the Control Design

- Confirm with key staff members that all infrastructure data and software are backed up prior to installation and/or maintenance tasks. Inspect backup logs to confirm that infrastructure data and software are successfully backed up.
- Confirm with key staff members that all application software is tested prior to installation in an environment separate from, but sufficiently similar to, production. Review test specifications and procedures to confirm that tests include functionality, security, availability and integrity condition, and any other vendor recommendations.
- Inspect the software configuration to confirm that key aspects have been addressed, including the modification of default passwords, initial application parameter settings relative to security and any other vendor defaults.
- Enquire whether and confirm that temporary access granted for installation purposes is monitored and that passwords are changed immediately after installation is completed. Inspect the application security settings to confirm compliance.
- Confirm with key staff members that only appropriately licensed software is tested and installed and that installations are performed in accordance with vendor guidelines. Identify instances where vendor guidelines were not followed, and confirm that vendors were consulted regarding the potential impact.
- Confirm with key staff members that an independent group (e.g., librarian) is granted access for the movement of the programs and data amongst libraries. Where applicable, inspect user access to the library management system.
- Trace all users with access to check-in/check-out programs and data from the libraries to their originating access request forms, and confirm approval by an appropriate senior staff member.
- Enquire with staff members whether acceptance procedures are enforced using objective acceptance critieria and whether acceptance criteria ensures that product performance is consistent with agreed-upon specifications and requirements. Review agreed-upon specifications and/or SLA requirements, and compare with acceptance procedures identifying areas where procedures are not adequately followed.
- Confirm with key staff members that access to maintenance activities over sensitive infrastructure components is logged and regularly reviewed by a responsible senior staff member.
- Review maintenance logs and confirm that all items have been recorded. Review relevant documentation (e.g., the log review matrix and periodic system security reports) to confirm that logs are reviewed on a regular basis.

AI3 Acquire and Maintain Technology Infrastructure (cont.)

Control Objective	Value Drivers	Risk Drivers
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.	• Monitored maintenance contracts • Effective maintenance processes • Operational change management for replacement of software	• Disruptions in production processing • Unauthorised access to sensitive software • Technology failing to support business needs • Violation of licence agreements

Test the Control Design

- Confirm with key staff members that maintenance of the installed system software process utilises the same process as application updates, where applicable. Inspect the planned system software maintenance and identify deviations from the normal process for application updates and/or exceptions to vendor procedures and guidelines.
- Confirm with key staff members that documentation of system software is maintained, kept current and updated with vendor documentation for all system maintenance activity.
- Inspect relevant documentation and identify areas where it is incomplete or out of date.
- Enquire of key staff members to confirm the process or method used to obtain timely notification of availability of vendor upgrades and/or patches (e.g., a specific vendor agreement, membership in a product user group, subscriptions to a trade journal).
- Inspect a sample of system software and confirm that upgrades and/or patches have been applied in a timely manner.
- Identify all deviations and/or exceptions.
- Enquire of key staff members whether the amount of maintenance being performed, the vulnerability to unsupported infrastructure, and future risks and security vulnerabilities are reviewed on a regular basis.
- Perform an assessment of these reviews and note areas where risks identified by the assessment have not been discussed by key staff members.
- Inspect maintenance tracking logs and feedback tools to ensure that the results of these reviews are communicated to the IT council or equivalent group for consideration within the infrastructure planning process.

Control Objective	Value Drivers	Risk Drivers
AI3.4 Feasibility Test Environment Establish development and test environments to support effective and efficient feasibility and integration testing of infrastructure components.	• Effective support for proving replacement of software • Detection of errors and issues before they impact production processing	• Business disruptions • Malicious damages

Test the Control Design

- Confirm with key staff members that an approach commensurate with strategic technology plans is designed that will enable the creation of suitable testing and simulation environments to help verify the feasibility of planned acquisitions or developments.

Take the following steps to test the outcome of the control objectives:
- Review acquisition infrastructure plans to confirm that they have been reviewed and approved and that risks, costs and benefits, and technical conformance have been considered. Inspect the plans to confirm sign-off by the IT council or equivalent.
- Confirm with key staff members that all security requirements associated with the application software installation and maintenance processes have been addressed and any new risks have been assessed and actioned.
- Confirm with the training department and key personnel who use sensitive infrastructure components that appropriate training has been provided.
- Confirm with key staff members that a plan and strategy are in place to guide infrastructure maintenance in line with change management procedures. Inspect relevant plan documentation to confirm that all aspects of the infrastructure maintenance requirements (including change requests, patches, upgrades, fixes) are included. Also confirm that the strategy and plan are in line with the organisation's technology direction, are reviewed in a timely manner and are approved by the responsible management.
- Confirm that the method used to segregate system environments into development and testing is adequate.
- Confirm that a test environment has been created that appropriately considers functionality, hardware and software configuration, integration and performance testing, migration between environments, version control, test data and tools, and security.

Take the following steps to document the impact of the control weaknesses:
- Identify performance problems that have impacted the overall performance of the system.
- Identify preventive maintenance problems that have impacted the overall performance of the system.
- Identify weaknesses in the setup, installation and maintenance of system software (including the selection of inappropriate system software parameters) that have jeopardised the security of the data and programmes being stored on the system.
- Identify weaknesses in the testing of system software that could jeopardise the security of the data and programmes being stored on the system.
- Identify weaknesses in the system software change control process that could jeopardise the security of the data and programmes being stored on the system.

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 Objective	Value Drivers	Risk Drivers
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.	• Consistent user and operations manuals • Support of user training • Enhanced service quality	• Overdue changes • Gaps between expectations and capability • Inappropriate priority given to different services provided • Inadequate budgets and resources to address gaps

Test the Control Design

- Confirm with key staff members that operational procedures and user documentation (including online assistance) have been defined and documented prior to implementation of new or upgraded automated systems or infrastructure.
- Inspect relevant documentation to confirm responsibility for the production of management, user and operational procedures in relation to the new or upgraded automated systems or infrastructure.

Control Objective	Value Drivers	Risk Drivers
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.	• Knowledge transfer within the organisation • Consistent quality over all affected teams • Efficient support for business • User manuals supporting business processes	• Increased reliance on key staff members • Problems in daily operations • Incidents encountered and repeated • Help desk overload

Test the Control Design

- Confirm through interviews with key staff members management's awareness and knowledge of the process to enable ownership and operation of the system (e.g., access approval, privilege management, segregation of duties, automated business controls, backup recovery, physical security, source document archival).
- Review training and implementation materials to determine if the defined process includes the required content.
- Confirm through interviews with key staff members that management is aware of and able to use the feedback mechanism to assess adequacy of the support documentation, procedures and related training.
- Interview business management personnel to assess their ability to use the system effectively.
- Walk through key system functions with business management personnel to identify areas where additional training would be helpful.
- Review and assess training materials for areas that are not covered or are unclear.

AI4 Enable Operation and Use (cont.)

Control Objective	Value Drivers	Risk Drivers
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.	• Knowledge transfer to stakeholders • Efficient and effective training • Optimised operation and system usage	• Inconsistent system usage • Insufficient documentation • Increased reliance on key staff members • Problems in daily operations • Training failing to meet user requirements • Help desk overload

Test the Control Design

- Interview key staff members about the user group's awareness and knowledge of the process to effectively and efficiently use the application system to support business processes (e.g., training and skills development, training materials, user manuals, procedure manuals, online help, service desk support, key user identification, evaluation).
- Review training and implementation materials to determine if the defined process includes the required content.
- Confirm through interviews with key staff members that the user is aware of and able to use the feedback mechanism to assess the adequacy of the support documentation, procedures and related training.

Control Objective	Value Drivers	Risk Drivers
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.	• Knowledge transfer to stakeholders • Efficient and effective training • Optimised operation and system support • Formally defined approaches for all stages of application development	• Insufficient documentation • Increased reliance on key staff members • Problems in daily operations • Training failing to meet operations or support requirements • Help desk overload

Test the Control Design

- Interview key staff members about the operation and technical support staff's awareness and knowledge of the process to effectively and efficiently deliver, support and maintain the application system and associated infrastructure according to service levels (e.g., training and skills development, training materials, user manuals, procedure manuals, online help, service desk scenarios).
- Review training and implementation materials to determine if the defined process includes the required content.
- Confirm through interviews with key staff members that operation and technical support personnel are aware of and able to use the feedback mechanism to assess adequacy of the support documentation, procedures and related training.
- Determine if operations and support staff members are involved in the development and maintenance of operations and support documentation.
- Identify areas where operational support procedures are not integrated with existing operational support procedures.

Take the following steps to test the outcome of the control objectives:
- For a selection of solution delivery projects, inspect documentation to determine that user and operational procedures manuals are in place.
- Assess management's knowledge to determine if members of management have directed the creation of management procedures for their business areas (e.g., access approval, privilege management, segregation of duties, automated business controls, backup/recovery, physical security, source document archival). Confirm that these procedures are integrated with existing management and control procedures, and investigate to determine if management is aware of discrepancies.
- Walk through new or upgraded applications with business management to identify areas where additional training is needed. Review and assess the training materials used.
- Inspect a selection of feedback documentation to determine if adequate feedback mechanisms have been used for developing support documentation, procedures and related training material.
- Assess users' involvement in the creation of user procedures for their business areas (e.g., training and skills development, training materials, user manuals, procedure manuals, online help, service desk support, key user identification, evaluation). Confirm that these procedures are integrated with existing user and control procedures (e.g., system inputs/outputs, system integration, error messages), and investigate to determine if users are aware of discrepancies.
- Walk through new or upgraded applications and infrastructure with operations management and technical support staff to identify areas where additional training would be helpful. Review and assess training materials for adequacy.
- Assess operation and technical support staff's involvement in the creation of operation and technical support staff procedures for their areas (e.g., training and skills development, training materials, user manuals, procedure manuals, online help, service desk scenarios). Confirm that these procedures (e.g., backup, restart/restore, reports/output distribution, emergency fixes, operator command/parameters, problem escalation) are integrated with existing operation and technical support staff members procedures. Investigate to determine if operation and technical support staff members are aware of discrepancies.

Take the following steps to document the impact of the control weaknesses:
- Assess the cost and operational inefficiency of inadequate training and/or user and operational procedures.
- Identify deficiencies in users, operations and training manuals.

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 Objective	Value Drivers	Risk Drivers
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.	• Optimised supplier relations • High-quality contribution to business and IT processes • Procurements supporting the achievement of desired business and IT goals	• Gaps in fulfiling requirements by suppliers • Commercial and contractual procurement exposures • Automated solutions not in line with the organisation's short- and long-term plans • Insufficient software quality in procured solutions • Lack of cost control

Test the Control Design

- Confirm through interviews with key staff members that the IT procurement process and acquisition strategy are aligned with the organisation's procurement policies and procedures (e.g., legislative requirements, compliance with the organisation's IT acquisition policy, licensing and leasing requirements, technology upgrade clauses, involvement of the business, total cost of ownership, acquisition plan for major acquisitions, recording of assets).
- Inspect project management policies and procedures to evaluate conformance with enterprise procurement policies and procedures.

Control Objective	Value Drivers	Risk Drivers
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.	• Defined supplier relationship objectives and goals • Efficiently managed procurement of resources • High-quality contribution to business and IT processes	• Lack of cost management • Gaps between business expectations and supplier capabilities • Undefined service costs incurred • Services failing to reflect business requirements • Lack of operational support

Test the Control Design

- Confirm through interviews with key staff members that the policies and standards are in place for establishing contracts with suppliers. The policies and standards should address, supplier-client responsibilities, supplier SLAs, monitoring and reporting against SLAs, transition arrangements, notification and escalation procedures, security standards, records management and control requirements and required supplier QA practices. Contracts should also include legal, financial, organisational, documentary, performance, security, auditability, intellectual property, responsibility and liability aspects.

AI5 Procure IT Resources (cont.)

Control Objective	Value Drivers	Risk Drivers
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.	• Contribution to new ideas and practices • A continuous contribution to the organisation's objectives beyond supplier SLAs	• Inappropriate supplier selection • Inadequate support for the achievement of the organisation's objectives • Gaps between supplier requirements and capabilities

Test the Control Design

- Confirm through interviews with key staff members that predefined, specified and established criteria (e.g., requirements definition, timetable, decision process) are used for supplier and acquisition selections.
- Inspect requests for information (RFIs) and requests for proposal (RFPs) to determine if the established criteria are defined.
- Enquire whether and confirm that software acquisitions include and enforce the rights and obligations of all parties (e.g., ownership and licensing of intellectual property; maintenance warranties; arbitration procedures; upgrade terms; and fitness for purpose, including security, escrow and access rights). For a selection of software acquisitions, inspect relevant documentation and determine if the contractual terms include the rights and obligations of all parties.
- Enquire whether and confirm that acquisitions of development resources include and enforce the rights and obligations of all parties (verify, for example, ownership and licensing of intellectual property; fitness for purpose, including development methodologies; languages; testing; quality management processes, including required performance criteria; performance reviews; basis for payment; warranties; arbitration procedures; human resource management; and compliance with the organisation's policies).
- Determine if legal advice has been obtained on resource development acquisition agreements regarding ownership and licensing of intellectual property.
- For a selection of acquisitions of development resources, inspect relevant documentation and determine if the contractual terms include the rights and obligations of all parties.
- Enquire whether and confirm that acquisitions of infrastructure, facilities and related services include and enforce the rights and obligations of all parties (e.g., service levels, maintenance procedures, access controls, security, performance review, basis for payment, arbitration procedures).
- For a selection of acquisition of infrastructure, facilities and related services, inspect relevant documentation and determine if the contractual terms include the rights and obligations of all parties.
- Enquire whether and confirm that RFIs and RFPs are evaluated in accordance with the approved process and criteria.
- Determine if documentary evidence is effectively maintained.

AI5 Procure IT Resources (cont.)

Control Objective	Value Drivers	Risk Drivers
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.	• Efficient and effective incident management • Systems operating as intended and not prone to disruption • Incidents able to be solved in a timely manner	• Software updates not available when needed • Software unable to support the business processes • Changes to the application unable to be applied as intended • System prone to problems and incidents, causing business disruptions

Test the Control Design

- Determine whether all acquisition agreements are verified.
- Review the agreements, compare them to policy documentation and determine whether they comply with company policy.
- Determine whether acquisitions are reviewed and approved by appropriate personnel and whether legal advice has been obtained.
- Inspect documentation of contract review and approval.
- Enquire whether common processes are established and used for acquisition of software, infrastructure and facilities.
- Perform a walk-through of the processes to determine if they operate effectively.
- Enquire whether rights and obligations of all parties to the acquisition are evaluated in the acquisition processes. These rights and obligations could include:
  - Approval
  - Service levels
  - Maintenance procedures
  - Access controls
  - Security
  - Performance review
  - Basis for payment
  - Arbitration procedures
- For a representative sample of acquisitions, determine if the rights and obligations of all parties are evaluated.
- Enquire whether the acquisition process adequately considers all relevant rights and obligations, which may include:
  - Ownership and licensing of intellectual property
  - Maintenance
  - Warranties and arbitration procedures
  - Upgrade terms
  - Fitness for purpose, including security
  - Escrow and access rights
- Determine if management reporting requirements associated with acquisitions are addressed.
- Enquire whether a quality assessment and acceptance process for all acquisitions has been established and used, and determine whether this process is effectively performed on all acquisitions before payment is made.
- Enquire whether all hardware and software acquisitions are recorded.
- Select a representative sample of acquisitions and verify that they are recorded in asset registers.

Take the following steps to test the outcome of the control objectives:
- For a selection of recent procurements, determine if the selection approach was responsive to the unique risks of the procurement (e.g., meets business functional and technical requirements, addresses risks identified in the risk analysis report, complies with procurement decisions).
- Inspect evidence of approvals at key decision points for a selection of IT procurements, including evidence of senior management sign-offs on sections that did not follow standard policies.
- For a selection of contracts, determine if only authorised suppliers were used.
- For a selection of supplier and acquisitions contracts, compare RFIs and RFPs with the predefined requirements, and determine if established criteria have been met.
- Enquire whether and confirm that software acquisitions include and enforce the rights and obligations of all parties (e.g., ownership and licensing of intellectual property; maintenance warranties; arbitration procedures; upgrade terms; fitness for purpose, including security; escrow and access rights). For a selection of software acquisitions, inspect relevant documentation and determine if the contractual terms include the rights and obligations of all parties.
- Enquire whether and confirm that acquisitions of development resources include and enforce the rights and obligations of all parties (verify, for example, ownership and licensing of intellectual property; fitness for purpose, including development methodologies; languages; testing; quality management processes, including required performance criteria; performance reviews; basis for payment; warranties; arbitration procedures; human resource management; compliance with the organisation's policies).
- Determine if legal advice has been obtained for resource development acquisition agreements regarding ownership and licensing of intellectual property.
- Enquire whether and confirm that acquisitions of infrastructure, facilities and related services include and enforce the rights and obligations of all parties (e.g., service levels, maintenance procedures, access controls, security, performance review, basis for payment, arbitration procedures). For a selection of acquisition of infrastructure, facilities and related services, inspect relevant documentation and determine if the contractual terms include the rights and obligations of all parties.
- Enquire whether and confirm that RFIs and RFPs have been evaluated in accordance with the approved process and criteria. Determine if documentary evidence is effectively maintained.

Take the following steps to document the impact of the control weaknesses:
- Assess the cost and time impact of IT procurement not being aligned with the organisation's procurement policies.
- Assess the cost and time impact of IT procurement not meeting business, legal and contractual requirements.
- Assess the legal implications of the supplier and acquisition selection process not complying with legal and contractual requirements.

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.

Control Objective	Value Drivers	Risk Drivers
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.	• An agreed-upon and standardised approach for managing changes in an efficient and effective manner • Changes reviewed and approved in a consistent and co-ordinated way • Formally defined expectations and performance measurement	• Inappropriate resource allocation • No tracking of changes • Insufficient control over emergency changes • Increased likelihood of unauthorised changes being introduced to key business systems • Failure to comply with compliance requirements • Unauthorised changes • Reduced system availability

Test the Control Design

- Enquire whether and confirm that the processes and procedures for handling change requests (including maintenance and patches) apply to applications, procedures, processes, system and service parameters, and the underlying platforms.
- Review the change management framework to determine if the framework includes:
  - The definition of roles and responsibilities
  - Classification (e.g., between infrastructure and application software) and prioritisation of all changes
  - Assessment of impact, authorisation and approval
  - Tracking of changes
  - Version control mechanism
  - Impact on data integrity (e.g., all changes to data files made under system and application control rather than by direct user intervention)
  - Management of change from initiation to review and closure
  - Definition of rollback procedures
  - Use of emergency change processes
  - Business continuity planning
  - Use of a record management system
  - Audit trails
  - Segregation of duties
- Enquire whether and confirm that processes and procedures for contracted services providers (e.g., infrastructure, application development, application service providers, shared services) are included in the change management process.
- Determine if the process and procedures include the contractual terms and SLAs.

AI6 Manage Changes (cont.)

Control Objective	Value Drivers	Risk Drivers
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.	• An agreed-upon and standardised approach for assessing impacts in an efficient and effective manner • Formally defined change impact expectations based on business risk and performance measurement • Consistent change procedure	• Unintended side effects • Adverse effects on capacity and performance of the infrastructure • Lack of priority management of changes

Test the Control Design

- Enquire whether and confirm that the change management process allows business process owners and IT to request changes to infrastructure, systems or applications.
- Enquire whether and confirm that requested changes are categorised (e.g., between infrastructures, operating systems, networks, application systems, purchased/packaged application software).
- Confirm through interviews with key staff members that requested changes are prioritised based on predefined criteria (e.g., business and technical needs for the change and legal, regulatory and contractual requirements).
- Enquire whether and confirm that change requests are assessed and documented in a structured method that addresses impact analysis on infrastructure, systems and applications.
- Enquire whether and confirm that security, legal, contractual and compliance implications are considered in the assessment process for the requested change and that business owners are involved.
- Enquire whether and confirm that each requested change is formally approved by the business process owners and IT technical stakeholders.
- Inspect a representative sample of change management requests to ensure that they were appropriately assessed, evaluated, prioritised and reviewed.

AI6 Manage Changes (cont.)

Control Objective	Value Drivers	Risk Drivers
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.	• An agreed-upon and standardised approach for managing changes in an efficient and effective manner • Formally defined emergency change expectations and performance measurement • Consistent procedure for emergency changes	• Inability to respond effectively to emergency change needs • Additional access authorisation not terminated properly • Unauthorised changes applied, resulting in compromised security and unauthorised access to corporate information

Test the Control Design

- Enquire whether and confirm that the overall change management process includes emergency change procedures (e.g., defining, raising, testing, documenting, assessing and authorising emergency changes).
- Inspect the documentation for a representative sample of emergency changes and, by interviewing key staff members, establish whether emergency changes are implemented as specified in the change management process.
- Confirm through interviews with key staff members that emergency access arrangements are authorised, documented and revoked after the change has been applied.
- Enquire whether and confirm that a post-implementation review of emergency changes is conducted.

Control Objective	Value Drivers	Risk Drivers
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.	• An agreed-upon and standardised approach for managing changes in an efficient and effective manner • Formally defined expectations and performance measurement • Consistent change procedure	• Insufficient allocation of resources • Changes not recorded and tracked • Undetected unauthorised changes to the production environment

Test the Control Design

- Enquire whether and confirm that there is an established process to allow requestors and stakeholders to track the status of requests throughout the various stages of the change management process.
- Enquire whether and confirm that the tracking and reporting system monitors the status of the change requests (e.g., rejected, approved but not initiated, approved, in process).
- Enquire whether and confirm that management reviews and monitors the detailed status of changes and overall state (e.g., aged analysis of change requests).
- Enquire whether and confirm that open and approved changes are closed in a timely manner, depending on priority.

AI6 Manage Changes (cont.)

Control Objective	Value Drivers	Risk Drivers
AI6.5 Change Closure and Documentation Whenever changes are implemented, update the associated system and user documentation and procedures accordingly.	• An agreed-upon and standardised approach for documenting changes • Formally defined expectations • Consistent change and documentation procedures	• Increased dependence on key individuals • Configuration documentation failing to reflect the current system configuration • Lack of documentation of business processes • Failure of updates for hardware and software changes

Test the Control Design
• Enquire whether and confirm that change documentation (e.g., operational procedures, configuration information, application documentation, help screens, training materials) is up to date. • Enquire whether and confirm that change documentation (e.g., pre- and post-implementation system and user documentation) is retained. • Enquire whether and confirm that business process documentation is updated for the changes implemented in hardware or software.

Take the following steps to test the outcome of the control objectives:
- For a sample of changes, confirm that the following have been approved by appropriate stakeholders (business process owners and IT management):
  - Request for change
  - Specification of change
  - Access to source programme
  - Programmer completion of change
  - Request to move source into test environment
  - Completion of acceptance testing
  - Request for compilation and move into production
  - Determination and acceptance of overall and specific security impact
- Develop a distribution process.
- Review change control documentation for inclusion of:
  - Date of requested change
  - Person(s) requesting
  - Approval of change request
  - Approval of change made—IT function
  - Approval of change made—users
  - Documentation update date
  - Move date into production
  - QA sign-off of change
  - Acceptance by operations
- For a selection of changes, review documentation to determine the existence of a version control mechanism.
- For a selection of changes related to contracted service providers, inspect implemented changes and determine if they follow vendor-provided instructions.
- Inspect a selection of changes and determine if requests have been categorised.
- Inspect a selection of changes and determine if changes have been prioritised based on predefined criteria.
- Inspect a selection of changes and determine if changes have been assessed in a structured method (e.g., security, legal, contractual and compliance implications are considered and business owners are involved).
- Inspect a sample of emergency changes and verify that they have been processed in accordance with the change management framework. Verify that procedures have been followed to authorise, document and revoke access after the change has been applied.
- Inspect a sample of emergency changes and determine if a post-implementation review has been conducted after the changes were applied. Consider implications for further application system maintenance, impact on development and test environments, application software development quality, documentation and manuals, and data integrity.
- Walk through the tracking and reporting system and verify that documentation is kept for rejected changes, the status of approved and in-process changes, and closed changes, and confirm with users to ensure that the status is current.
- Inspect a selection of change status reports to determine if an audit trail is used to track changes from inception to disposition.
- Inspect a sample of change status reports to determine if performance metrics are used to aid management's review and monitoring.
- Inspect a sample of changes to determine if change documentation has been retained in accordance with the appropriate retention period.
- Inspect business process manuals to determine if they have been updated with new or improved functionality changes in hardware and software.
- Select a sample of changes and assess the quality of co-ordination with third parties.
- Confirm the process of assessing the performance of the change management process. Assess any potential improvements identified that resulted in recommendations to IT management to improve the change management process.

Take the following steps to document the impact of the control weaknesses:
- Assess the time and cost of lack of formal change management standards and procedures (e.g., improper resource allocation, unclear roles and responsibilities, security breaches, lack of rollback procedures, lack of documentation and audit trails, inadequate training).
- Assess the time and cost of lack of formal impact assessment to prioritise and authorise changes.
- Assess the time and cost of lack of formal emergency change standards and procedures (e.g., compromised security, failure to properly terminate additional access authorisations, unauthorised access to corporate information).
- Assess the impact (e.g., insufficient allocation of resources, lack of priority management, changes not recorded and tracked, unauthorised changes to the productive environment undetected) of lack of tracking and reporting changes.
- Assess the impact (e.g., increased dependence on key individuals, configuration documentation not reflecting the current system configuration, documentation lacking business processes, failure of updates for hardware and software changes) of lack of system and user documentation.
- Assess the impact (e.g., failure of systems to meet end users' needs, lack of cost and resource control for changes, loss of business focus for changes, failure of return on investments to meet management's expectations, unavailability of new systems for the business processes) of lack of evaluation of the change process.

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.

Control Objective	Value Drivers	Risk Drivers
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.	• Consistent development of new skills • Enhanced training for effective and efficient job performance • Familiarisation with new or modified systems	• Failure to promptly detect problems with systems or their use • Gaps in knowledge to perform required duties and activities • Errors resulting from new projects

Test the Control Design

- Enquire whether and confirm that a training plan is part of the overall project master plan for development projects.
- Enquire whether and confirm (e.g., through interviews with key staff members or inspection of project plan) that the training plan identifies and addresses impacted groups (e.g., business end users, IT operations, support and IT application development training, service providers).
- Enquire whether and confirm that alternative training strategies are considered to ensure that a cost-effective approach is selected and incorporated in the training framework.
- Enquire whether and confirm that there is a process to verify compliance with the training plan.
- Inspect training documentation to determine compliance to the training plan (e.g., list of staff members invited to training, attendees list, evaluation forms for the achievement of learning objectives and other feedback).
- Enquire whether and confirm that there is a process of monitoring training to obtain feedback that could lead to potential improvements in the system.
- Enquire whether and confirm that planned changes are monitored to ensure that training requirements are considered and suitable plans are created.

AI7 Install and Accredit Solutions and Changes (cont.)

Control Objective	Value Drivers	Risk Drivers
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.	• Commitment of key stakeholders • Minimised business interruptions resulting from system processing failure	• Insufficient testing by automated test scripts • Performance problems undetected • Lack of cost control over testing activities • Undefined testing roles and responsibilities

Test the Control Design

- Enquire whether and confirm that a test plan is developed and documented in accordance with the project quality plan and relevant organisational standards and that it is communicated to appropriate business owners and IT stakeholders.
- Enquire whether and confirm that the test plan reflects an assessment of the project's risks and that all functional and technical testing requirements are included.
- Enquire whether and confirm that the test plan identifies resources to execute the tests and evaluate test results.
- Confirm that stakeholders are consulted on resource implications of the test plan.
- Enquire whether and confirm that the test plan considers test preparation, including site preparation; training requirements; installation or update of a defined test environment; planning/performance/documentation/retention of test cases; error and problem handling, correction and escalation; and formal approval.
- For a sample of test plans, inspect documentation to determine if appropriate test phases are performed.
- Enquire whether and confirm that the test plan establishes clear criteria for measuring the success of undertaking each testing phase and that consultations with the business process owners and IT stakeholders are considered in defining the success criteria.
- Determine if the plan establishes remediation procedures when the success criteria are not met (e.g., in case of significant failures in a testing phase, the plan provides guidance on whether to proceed to the next phase, stop testing or postpone implementation).
- Enquire whether and confirm that test plans are approved by stakeholders, including business process owners and IT, as appropriate. Examples of other stakeholders are application development managers, project managers and business process end users.

AI7 Install and Accredit Solutions and Changes (cont.)

Control Objective	Value Drivers	Risk Drivers
AI7.3 Implementation Plan Establish an implementation and fallback/backout plan. Obtain approval from relevant parties.	• An agreed-upon and standardised approach for implementing changes in an efficient and effective manner • Formally defined expectations and performance measurement • Effective recovery in the event of implementation failure	• Improper resource allocation to ensure effective implementation of changes • Security breaches

Test the Control Design

- Confirm for a representative sample of projects that the implementation plan has been reviewed and approved.
- Enquire whether and confirm that an implementation plan has been created that includes the broad implementation strategy, the sequence of implementation steps, resource requirements, interdependencies, criteria for management agreement to the production implementation, installation verification requirements and transition strategy for production support.
- Select a representative sample of projects and validate that the implementation plan is aligned with the business change management plan.
- Enquire whether and confirm that third parties are committed to be involved in each step of the implementation.
- Enquire whether and confirm that fallback and recovery processes are identified and documented in the implementation plan.

Control Objective	Value Drivers	Risk Drivers
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.	• Minimised business interruptions in production	• Insufficient testing using automated test scripts • Performance problems undetected • System security compromised

Test the Control Design

- Enquire whether and confirm that the test environment is set up to mirror the production environment (factors include workload/stress, operating systems, necessary application software, database management systems, network and computing infrastructure).
- Enquire whether and confirm that the test environment is incapable of interacting with production environments.
- Enquire whether and confirm that a test database exists.
- Evaluate the existence and quality of a data-sanitising process in creating a test database.
- Assess protection measures and the authorisation of access to the test environment.
- Enquire whether and confirm that a process exists and is complied with to manage retention or disposal of test results.
- Enquire whether and confirm that the retention process meets or exceeds regulatory or compliance requirements.

AI7 Install and Accredit Solutions and Changes (cont.)

Control Objective	Value Drivers	Risk Drivers
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.	• Improper components detected and removed from production • New system operating as intended and supporting the business processes	• Old systems not available when needed • Unreliable system and conversion results • Subsequent processing interruptions • Data integrity issues

Test the Control Design

- Confirm (e.g., through interviews with key staff members or inspection of policies and procedures) that data conversion and infrastructure mitigation plans exist, and consider the following: hardware, networks, operating systems, software, transaction data, master files, backups and archives, interfaces with other internal and external systems, procedures, system documentation, etc.
- Through interviews with key staff members, enquire about the timing and completeness of conversion cutover.
- Enquire whether and confirm that a backup is taken prior to conversion, audit trails are maintained, and a fallback and recovery plan exists.

Control Objective	Value Drivers	Risk Drivers
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.	• Achieved system performance • Effective cost control • Increased customer confidence	• Waste of resources • Degraded overall security • Changes impacting system performance and availability

Test the Control Design

- Enquire whether and confirm that testing of changes is developed with independence (separation of duties) and conducted only in the test environment.
- Enquire whether and confirm that test scripts exist to validate security and performance requirements.
- Confirm through interviews that fallback or backout plans are prepared and tested prior to changes being promoted into production.

AI7 Install and Accredit Solutions and Changes (cont.)

Control Objective	Value Drivers	Risk Drivers
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.	• Minimised business interruptions in production • Critical data flows protected • Deviations from expected service quality identified • Application meeting usability requirements	• Performance problems undetected • Business rejection of delivered capabilities

Test the Control Design
• Confirm that key stakeholders are considered in the final acceptance testing activities. • Enquire whether and confirm that in the final acceptance stages, success criteria are identified in the testing plan. • Enquire whether and confirm that appropriate documentation for review and evaluation exists. • Enquire of key stakeholder whether the documentation and presentation of final acceptance testing results are complete and timely.

AI7 Install and Accredit Solutions and Changes (cont.)

Control Objective	Value Drivers	Risk Drivers
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.	• An agreed-upon and standardised approach for promoting changes into production in an efficient and effective manner • Formally defined expectations and performance measurement • Consistent change procedure	• Segregation of duties violations • Systems exposed to fraud or other malicious acts • No rollback to previous application system version possible

Test the Control Design

- Review procedures for program transfer to verify that a formal process exists that requires documented approval from user management and system development.
- Confirm that the approval process identifies effective dates for promotion of new systems, applications or infrastructure to production, as well as for the retirement of old systems, applications and infrastructure.
- Enquire whether and confirm that the approval process includes a formal documented sign-off from business process owners, third parties and IT stakeholders as appropriate (e.g., development group, security group, database management, user support and operations group).
- Confirm procedures for updating copies of system documentation and relevant contingency plan.
- Enquire of key staff members concerning procedures for updating all source program libraries and procedures for labelling and retaining prior versions.
- Enquire of key staff members regarding required procedures for obtaining from the acceptance testing function the media used for implementation.
- Enquire of key staff members whether automated software distribution is controlled and whether there are checks in the distribution process that verify that the destination environment is of the correct standard implementation and version.
- Evaluate the effectiveness of the control to verify that distribution occurs only to authorised and correctly identified destinations.
- Enquire of key staff members whether a formal log is kept of what software and configuration items have been distributed, to whom they have been distributed, where they have been implemented, and when each has been updated.
- Enquire of key staff members concerning procedures for promptly updating all program copies and procedures for providing implementation order instructions in advance to all impacted locations.

AI7 Install and Accredit Solutions and Changes (cont.)

Control Objective	Value Drivers	Risk Drivers
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.	• An agreed-upon and standardised approach for post-implementation reviews • Consistent and transparent review procedure • Efficient use of organisational resources • Improved end-user satisfaction	• Failure to identify that systems do not meet end users' needs • Return on investments failing to meet management's expectations

Test the Control Design

- Confirm through interviews with key staff members that post-implementation procedures have been established.
- Confirm through interviews with key staff members that business process owners and IT technical management are involved in the selection of metrics for measuring success and achievement of requirements and benefits.
- Confirm through interviews with key staff members that the form of the post-implementation review is in accordance with the organisational change management process and that business process owners and third parties are involved, as appropriate.
- Confirm through interviews with key staff members that requirements for post-implementation review arising from outside business and IT are considered.
- Confirm through interviews with key staff members that an action plan exists to address issues identified in the post-implementation review and that business process owners and IT technical management are involved in the development of the action plan.

Take the following steps to test the outcome of the control objectives:

- Inspect the training plan to determine if it clearly identifies learning objectives, resources, key milestones, dependencies and critical path tasks. Confirm that the training plan considers alternative training strategies depending on the business needs.
- Inspect training plan documentation to confirm that:
  – It identifies the staff members who must be trained
  – The training was delivered in a timely manner
  – A cost-effective approach is selected and used (e.g., train the trainer, end-user accreditation, intranet-based training)
  – Feedback (e.g., evaluation forms, comment sheet) is received and used in identifying areas of potential improvements in the system
  – Planned changes are considered training requirements
  – It aligns with the project quality plan and relevant organisational standards
  – Test plans were communicated to appropriate business owners and IT stakeholders
- Inspect test documentation to determine if testing was performed based on the project's risk assessment. Confirm that all functional and technical testing requirements are covered (e.g., performance, stress, usability, pilot and security testing) and that the test plan addressed any requirement for internal or external accreditation.
- Inspect test documentation to determine if resources were identified for executing the test and evaluating the results (e.g., construction of test environments and staff members for the test group, including potential temporary replacement of test staff members in the production or development environments).
- Review a sample of test scripts to ensure that they adequately address each test criterion.
- For a sample of system development, implementation or modification projects, inspect test documentation to determine if appropriate test phases are performed (e.g., unit test, system test, integration test, user acceptance test, performance test, stress test, data conversion test, security test, operational readiness test).
- For a sample of test plans, inspect documentation to determine if the:
  – Criteria for measuring success for each testing phase are considered
  – Test plans are approved
  – Test database uses only sanitised data and is protected against disclosure
- Inspect conversion plans for adequacy, and confirm with the data owners the results of the conversion for completeness and integrity.
- Inspect and evaluate documentation for fallback/backout plans.
- Verify that error logs include audit trails to facilitate timely bug fixing and remediation.
- Review the final acceptance testing activities to evaluate whether the scope effectively covered all components and effectively addressed the acceptance criteria.
- Review acceptance testing results and evaluate the effectiveness of their interpretation and presentation.
- Inspect results of testing to verify that formal sign-off exists prior to promotion to production.
- Inspect source program libraries to verify that they are updated to the current versions and that prior versions are clearly labelled and retained for a reasonable period of time.
- Evaluate the effectiveness of the control to verify that distribution occurs only to authorised and correctly identified destinations.
- Inspect the log and verify that a procedure has been implemented to ensure its integrity and completeness.
- Physically inspect implementation orders/instructions on file.
- Select a sample of system development, implementation or modification projects and inspect change documentation to determine if management sign-off is performed to ensure that the change is authorised, tested and properly documented before software is released to production.
- Walk through the archive environment, and physically inspect archived versions and documentation.
- Assess the effectiveness of the change handover process in ensuring that only authorised, tested and documented changes are accepted in production.
- Assess the effectiveness of the process in ensuring that software implemented is unchanged from what has been tested.
- Select a sample of build requests and inspect documentation to determine if media preparation is based only on formal build requests.
- Confirm the effectiveness of the backout or reversal procedures.
- Confirm that a distribution audit trail includes the software and configuration items that have been distributed, to whom they have been distributed, where they have been implemented and when each has been updated.
- Confirm that automated software distribution occurs only to authorised and correctly identified destinations.
- Confirm that post-implementation procedures identify, assess and report on the extent to which business requirements have been met; expected benefits have been realised; the system is considered usable; internal and external stakeholders' expectations are met; unexpected impacts on the organisation may have occurred; key risks are mitigated; and the change management, installation and accreditation processes were performed effectively and efficiently.
- Enquire whether and confirm that requirements for post-implementation review arising from outside business and IT are considered.
- For a sample of system development or implementation projects, confirm that outside business and IT requirements (e.g., internal audit, enterprise risk management, regulatory compliance) are included in the post-implementation review.

- Select a sample of system development and implementation projects and confirm that the post-implementation plan includes an action plan to address the issues identified. Confirm that business process owners and IT technical management are involved in the development of action plans.
- Assess the effectiveness of the process for verification of success or failure of changes.
- Assess the configuration inventory to determine if changes are reviewed and accepted.
- Identify:
  - Any changes that were made without approval
  - Any changes not accounted for
  - Current libraries (source and object) not reflecting the most recent changes
  - Change control procedure variances
- Assess the impact of failed or erroneous changes.
- Assess the impact of late or delayed changes.

Take the following steps to document the impact of the control weaknesses:

- Assess the cost and operational inefficiency (e.g., failure to detect problems promptly, gaps in knowledge to perform the duties) of lack of training.
- Assess the impact (e.g., insufficient testing by automated test scripts, failure to detect performance problems, lack of cost control, undefined roles and responsibilities) due to the lack of a test plan.
- Assess whether the implementation plan has been reviewed and approved by major stakeholders to ensure that appropriate commitment exists throughout the life of the project.
- Assess the existence of a test environment to mirror production and provide a reliable future state for changes to business operations.
- Assess the data conversion plan for completeness to ensure that it includes audit trail, rollback procedures and fallback procedures.
- Assess changes that are tested independently in accordance with the defined test plans prior to migration into production.
- Assess the test plans to include a test to validate security and performance requirements.
- Assess the outcome of the testing process to identify errors requiring timely remediation prior to promotion to production.
- Assess the impact of a the lack of a post-implementation plan.

Page intentionally left blank

Appendix IV—Deliver and Support (DS)

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

APPENDIX IV—DELIVER AND SUPPORT (DS)

PROCESS ASSURANCE STEPS

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.

Control Objective	Value Drivers	Risk Drivers
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.	• Clarified IT service responsibilities and IT objectives aligned with business objectives • Improved communication and understanding between business customers and IT service providers • Consistency promoted in service levels, service definitions, and service delivery and support	• Gaps between expectations and capabilities, leading to disputes • Customers and providers not understanding their responsibilities • Inappropriate priority given to different services provided • Inefficient and costly operational service

Test the Control Design

- Inspect SLA policies and procedures for the alignment of SLA objectives and performance measures with business objectives and IT strategy.
- Enquire whether and confirm that policies exist for the alignment of SLA objectives and performance measures with business objectives and IT strategy.
- Inspect the service catalogue and verify that it incorporates service requirements, service definitions, SLAs, OLAs and funding sources.
- Enquire of staff members accountable for SLA escalation and resolution to determine whether the procedures or methods established reasonable service levels in responding to issues.
- Inspect a sample of relevant changes and verify that changes were implemented in accordance with the change management process.
- Inspect the design of the service improvement programme for standards to measure performance.

DS1 Define and Manage Service Levels (cont.)

Control Objective	Value Drivers	Risk Drivers
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.	• IT service objectives aligned with business objectives • IT operational service based on correct requirements and priorities • Incidents linked to services they impact, enabling incident response to be effectively prioritised	• Inappropriately delivered services • Incorrect priority for provided services • Misunderstood impact of incidents, leading to slow response and significant business impact • Different interpretations and misunderstanding of IT services provided

Test the Control Design

- Enquire whether and confirm that a process exists for developing, reviewing and adjusting the service catalogue or portfolio of services.
- Confirm the existence of a management process to ensure that the service catalogue or portfolio is available, complete and up to date.
- Inspect the service catalogue or portfolio process to verify that it is reviewed on a regular basis.

Control Objective	Value Drivers	Risk Drivers
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.	• Service responsibilities and IT objectives aligned with business objectives • Service quality enhanced due to proper understanding and alignment of service delivery • Service efficiency increased and costs reduced due to efficient deployment of IT services based on real needs and priorities	• Failure to meet customer service requirements • Inefficient and ineffective use of service delivery resources • Failure to identify and respond to critical service incidents

Test the Control Design

- Enquire whether and confirm that stakeholders agree to, record and communicate the SLA, and what is included in the format and contents.
- Inspect the format of the SLA's content to verify that it includes exclusions, commercial arrangements and OLAs.
- Inspect the SLA management process to verify that it measures SLAs (qualitative and quantitative) and monitors the SLA objectives.
- Inspect SLA's for approval and appropriate signatures.
- Observe and review the SLA review process to evaluate its adequacy.
- Verify that the process for improvements or adjustments to SLAs is based on performance feedback and changes to customer and business requirements.
- Enquire of key staff members whether services are being rendered that are not documented in the SLA.

DS1 Define and Manage Service Levels (cont.)

Control Objective	Value Drivers	Risk Drivers
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.	• Operational services aligned with SLAs and, therefore, to business needs • Optimisation of operational resources by standardisation and alignment with service requirements • Cost reduction by optimised use of resources and fewer service incidents	• Failure of the provided services to meet the business requirements • Gaps in technical understanding of services leading to incidents • Inefficient and costly use of operational resources

Test the Control Design

- Enquire whether and confirm that a process has been defined to develop, manage, review and adjust OLAs.
- Inspect the SLA(s) and confirm that the OLA supports the technical requirements of the respective SLA(s).
- Obtain a representative sample of OLAs and evaluate whether the OLAs contain operable and optimal definitions of delivery of services.

Control Objective	Value Drivers	Risk Drivers
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.	• Users able to monitor service level performance based on reliable information • The values of IT services communicated within the enterprise • Consistent communication between relevant parties	• Lack of defined measures important to the organisation • Unidentified underlying service problems and issues • Dissatisfied users due to lack of information, irrespective of quality of service

Test the Control Design

- Through interviews with key staff members responsible for monitoring service level performance, determine reporting criteria.
- Obtain samples of SLA performance reporting, and verify distribution.
- Inspect reviews for forecast and trends in service level performance.

DS1 Define and Manage Service Levels (cont.)

Control Objective	Value Drivers	Risk Drivers
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.	• Delivered IT services aligned with changing business needs • Weaknesses in existing service agreements identified and corrected	• Commercial and legal requirements not met due to out-of-date contracts • Services not meeting changed requirements • Financial losses and incidents due to misaligned services

Test the Control Design

- Inspect the SLAs, compare the UCs, and determine effectiveness and currency of changes.
- Obtain a walk-through of SLA documentation requirements.
- Review SLAs and UCs, and confirm that alignment with business objectives is evaluated on a regular basis.

Take the following steps to test the outcome of the control objectives:
- Enquire of senior management, representing the business and IT functions, about their involvement in the design and approval of the SLA framework.
- Enquire of key staff members if performance critieria have been formalised to support and measure achievement of SLA objectives, and if a process is in place to monitor and report the attainment of the objectives.
- Inspect the internal and external performance SLAs, and compare actual results for alignment with the expected SLA requirements.
- Confirm that the IT service objectives align with business objectives, and formally define expectations and performance measurements.
- Inspect service records to ascertain reasons for non-performance, and validate that a performance improvement programme is in place.
- Analyse the historical performance records, and determine that results are tracked against prior service improvement commitments.
- Enquire of key staff members whether stakeholders agree to, record and communicate the SLA and what is included in the format and contents.
- Inspect the format of contents of the SLAs to verify that they include exclusions, commercial arrangements and OLAs.
- For a sample of past and in-process SLAs, determine that content includes:
  - Definition of service
  - Cost of service
  - Quantifiable minimum service level
  - Level of support from the IT function
  - Availability, reliability and capacity for growth
  - Change procedure for any portion of the agreement
  - Continuity planning
  - Security requirements
  - Written and formally approved agreement between the provider and user of the service
  - Effective period and new period review/renewal/non-renewal
  - Content and frequency of performance reporting and payment for services
  - Realistic charges compared to history, industry and best practices
  - Calculation for charges
  - Service improvement commitment
  - Formal approval of the user and provider
- Confirm that appropriate users are aware and understand SLA processes and procedures.
- Inspect SLAs to verify that the OLAs and UCs support the technical requirements of the SLAs and are delivered in an optimal manner.
- Select a sample of SLAs, and confirm that resolutions procedures for inappropriate service delivery, specifically non-performance, are included and being met.
- Inspect the service catalogue and ascertain that all services are defined properly.
- Enquire whether and confirm that distinct IT services to which costs will be allocated have been defined and documented.
- Ascertain whether business process owners have knowledge of those IT services that support their business process.
- Inspect any documentation available that identifies business processes and their supporting infrastructure or IT services, and determine whether the mapping is accurate and complete. This can be accomplished, for example, by comparing the mapping to the organisational chart, lines of business, etc.
- Enquire of business process owners and IT service owners whether they have agreed on a mapping of IT services to business processes.
- Enquire of business process owners and users regarding their degree of satisfaction with IT services provided to identify potential weak areas. Such enquiries may be conducted in person or via an anonymous survey.
- Inspect documentation that relates to the mapping between IT service areas and business processes to determine if the operational aspects of the mapping are in place (e.g., SLAs should be examined for appropriateness).

Take the following steps to document the impact of the control weaknesses:
- Benchmark SLAs against similar organisations or appropriate international standards/recognised industry best practices.
- Determine the existence of gaps between service level expectations and delivered services through inquiry and review of documented disputes and fee discounts.
- Determine if services result in frequent fee surcharges and base fee overruns.
- Determine if service level failures were escalated and resolved in a timely manner.
- Determine if the service catalogue is up to date and aligned with business goals.
- Assess the adequacy of proposed service improvements in comparison with the cost-benefit analysis.
- Determine that gaps in expected services are appropriately prioritised and address control requirements for managing services based on service characteristics and business requirements.
- Assess the adequacy of the provision, describing, co-ordinating and communicating the relationship between the provider and user of information services.

- Assess the adequacy of the provider's ability to meet improvement commitments in the future.
- Enquire of key management staff members whether service level framework provides assurance that SLAs and contracts are current and aligned with business objectives.
- Determine whether reports on achievement of the specified service performance are appropriately used by management to ensure satisfactory performance.
- Determine whether reports of all problems encountered are appropriately used by management to ensure that corrective actions are taken.
- Assess the services provided to determine whether operational agreements align with SLAs.
- For selected categories of reported SLA information, determine the existence of inconsistency of service delivery.
- Assess users' satisfaction levels with the current service level process and actual agreements.
- Assess the service level measurement criteria, and determine the effectiveness of the communication flow between all relevant parties.
- Review SLAs to determine qualitative and quantitative provisions confirming that obligations are defined and being met.
- Assess management's ongoing review of and corrective action for service level reporting.
- Determine whether financial losses incurred are reflective of insufficient service quality.
- Verify the service catalogues' completeness by reviewing and reconciling change requests, network plans, server documentation, incident records, timesheets and other means of communication
- Enquire of IT service leaders regarding daily duties and responsibilities to ascertain whether those duties provide sufficient coverage of IT infrastructure.
- Corroborate outcomes of discussions with outputs of data centre tours, asset registries, network diagrams or other infrastructure inventories, and identify infrastructure not linked to an IT leader.
- Inspect asset registries, network diagrams or other infrastructure inventories, and ascertain the percentage of assets that are not assigned to an IT service area.
- Document the criticality of those assets in light of the service provided.
- Inspect documentation identifying IT services and business processes, and ascertain the degree of unallocated IT service areas.
- Document the criticality of those service areas in light of the affected business processes.

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 Objective	Value Drivers	Risk Drivers
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.	• Centralised service supplier overview to support supplier decision making • Preferred suppliers identified for future acquisitions • Supplier management resources focused on critical suppliers	• Unidentified significant and critical suppliers • Inefficient and ineffective usage of supplier management resources • Unclear roles and responsibilities leading to miscommunications, poor services and increased costs

Test the Control Design

- Enquire whether and confirm that a register of supplier relationships is maintained.
- Obtain and inspect supplier relationship criteria for reasonableness and completeness of categorisations by supplier type, significance and criticality.
- Determine if the supplier categorisation scheme is sufficiently detailed to categorise all supplier relationships based on the nature of contracted services.
- Verify whether past histories on supplier selection/rejection are kept and used.
- Inspect the register of supplier relationships to ensure that it is up to date, appropriately categorised and sufficiently detailed to ensure that it provides a foundation for monitoring of existing suppliers.
- Inspect a representative sample of supplier contracts, SLAs and other documentation to ensure that they correspond with the supplier register.

Control Objective	Value Drivers	Risk Drivers
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).	• Relationships promoted that support the overall enterprise objectives (both business and IT) • Effective and efficient communication and problem resolution • Clear ownership of responsibilities between customer and supplier	• Supplier not responsive or committed to the relationship • Problems and issues not resolved • Inadequate service quality

Test the Control Design

- Inspect service supplier documentation for evidence of formalised roles and responsibilities, and determine if supplier management roles have been documented and communicated within the organisation.
- Determine if policies exist to address the need for formal contracts, definition of content of contracts, and assignment of owner or relationship manager responsibilities for ensuring that contracts are created, maintained, monitored and renegotiated as required.
- Assess if the assignment of supplier management roles is reasonable and based on the level and technical skills required to effectively manage the relationship.

DS2 Manage Third-party Services (cont.)

Control Objective	Value Drivers	Risk Drivers
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.	• Compliance with legal and contractual requirements • Reduced incidents and potential losses • Identification of low-risk, well-managed suppliers	• Non-compliance with regulatory and legal obligations • Security as well as other incidents • Financial losses and reputational damage because of service interruption

Test the Control Design

- Enquire whether risks associated with the inability to fulfil the supplier contracts are defined.
- Enquire whether remedies were considered when defining the supplier contract.
- Inspect contract documentation for evidence of review.
- Enquire of key staff members whether a risk management process exists to identify and monitor supplier risk.
- Determine if policies exist requiring independence within the vendor sourcing and selection process, and between vendor and management personnel within the organisation.

Control Objective	Value Drivers	Risk Drivers
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.	• Timely detection of service level non-compliance • Benefits of service contract realised • Costs controlled • Costly disputes and possible litigation avoided	• Undetected service degradation • Inability to challenge costs and service quality • Inability to optimise choice of suppliers

Test the Control Design

- Select a sample of supplier invoices, determine if they identify charges for contracted services, as specified within service contracts, and assess the reasonableness of charges compared to various internal, external and industry comparable performance.
- Inspect a sample of supplier service reports to determine if the supplier regularly reports on agreed-upon performance criteria and if performance reporting is objective and measurable and in alignment with defined SLAs and the supplier contract.

Take the following steps to test the outcome of the control objectives:

- For a sample of suppliers, assess if supplier records are aligned to the defined catogorisation scheme used to identify and categorise all supplier relationships.
- Obtain and validate the list of supplier relationship criteria for completeness, and review suppliers' records against the catogorisation scheme used to identify and categorise all supplier relationships. Assess if supplier type, significance and criticality of services provided have been documented.
- Obtain a register of suppliers, and verify the accuracy of data through inspection of a sample of service contracts.
- Obtain a register of suppliers, and verify the accuracy of data. Consideration should be given to organisational changes or recent changes in the IT landscape that would require changes in the supplier relationship criteria.
- Determine if supplier documentation is sufficiently detailed to identify methods of communication, prioritisation of services and escalation procedures, minimum service levels, and operational objectives.
- Ascertain if documentation clearly delineates responsibilities between the service provider and the user organisation.
- Determine if service supplier documentation is centrally managed and maintained and if a process exists for the periodic review and updating of documents.
- Perform a detailed review of each third-party contract to determine the existence of qualitative and quantitative provisions confirming obligations, including provisions for co-ordinating and communicating the relationship between the provider and user of information services.
- Determine if policies exist for management's periodic review of service supplier reporting, and select a sample of supplier reports for evidence of management's review.
- Obtain and inspect service supplier incident reports for existence, and determine if incidents were categorised and escalated according to agreed-upon levels of severity and if they were tracked and communicated within the organisation until resolved. Reported incidents should include communication to supplier management and users of the services.
- Verify that goals and expected service levels are periodically reviewed to ensure that they continue to support current business requirements and that suggested changes are communicated clearly to service suppliers.
- Inspect the supplier register for assignment of a relationship manager, and obtain and inspect evidence of a service supplier communication process.
- Obtain and review contracts for existence of clauses relating to third-party reviews, and determine if management has obtained and reviewed reports from such reviews.
- For a sample of suppliers, inspect available documentation to determine if supplier risk has been considered and if identified risk has been addressed/mitigated.
- For a sample of supplier relationships, determine if the following have been addressed within the supplier contract:
  - Security requirements
  - Non-disclosure guarantees
  - Right to access and right to audit
  - Formal management and legal approval
  - Legal entity providing services
  - Services provided
  - SLAs, both qualitative and quantitative
  - Cost of services and frequency of payment for services
  - Resolution of problem process
  - Penalties for non-performance
  - Dissolution process
  - Modification process
  - Reporting of service—content, frequency and distribution
  - Roles between contracting parties during the life of the contract
  - Continuity assurances that services will be provided by the vendor
  - Communications process and frequency between the user of services and provider
  - Duration of contract
  - Level of access provided to vendor
  - Regulatory requirements
- For a sample of suppliers, determine if services have been assessed for criticality to the organisation, and determine if continuity of services has been addressed within the supplier contract, including contingency planning by the supplier, to ensure continuous service to the organisation.
- For a sample of supplier relationships, determine if legal counsel and management approved the supplier contracts.
- Select a sample of supplier invoices, determine if they identify charges for contracted services, as specified within service contracts, and assess the reasonableness of charges compared to various internal, external and industry comparable performance.
- Inspect a sample of supplier service reports to determine if the supplier regularly reports on agreed-upon performance criteria and if performance reporting is objective, measurable and in alignment with defined SLAs and the supplier contract.

Take the following steps to document the impact of the control weaknesses:

- Through inquiry of user and IT management and benchmarking of the organisation to similarly sized organisations and organisations within the same industry, identify any supplier relationships that have been excluded from the supplier register. Consider the following supplier relationships:
  - Private branch exchange (PBX) suppliers
  - Paper and form suppliers
  - Maintenance support suppliers
  - Offsite data storage and hot-site services providers
  - Service organisations providing data processing (e.g., ASP, co-location)
  - External software developers and quality assurance
- Inquire of supplier management to ascertain if they are knowledgeable of the nature of the service supplier relationship and contracted services.
- Inspect a sample of service supplier billings for out-of-scope billings, and determine the involvement of supplier management in reviewing and approving the overage.
- For a sample of service suppliers, obtain the supplier's reported performance metrics, and review for deviations from agreed-upon performance objectives. Determine if supplier management was aware of any deviations and the reasonableness of actions taken for deviation (e.g., establishment of action plan, service fee penalties for non-performance).
- For a sample of supplier relationships, determine if the level of services compares to the stated contractual obligations. For changes in the supplier relationships, determine if the risk assessments has been updated and if the supplier contract has been appropriately modified.
- Inspect a sample of supplier-reported performance metrics, and identify where performance objectives have not consistently been attained.
- Determine if management has identified and assessed the performance failures, and if an assessment has been performed, re-evaluate the relationship or evaluate the need for modifying the relationship.
- For supplier relationships with the greatest impact on the organisation, determine if contingency plans exist for the recovery or secondary sourcing of contracted services.
- Determine the availability of supplier third-party assessments (e.g., SAS No. 70, ISA 402 or attestation reports) or audit reports and whether management has received and reviewed the reports. For reported control deficiencies (i.e., report qualifications, testing exceptions), determine if management has discussed the deficiencies with the supplier and if an action plan has been implemented. Through review of past or subsequent reports, determine if the supplier promptly remediates control deficiencies.
- Determine if key suppliers are included in the annual risk assessment and audit planning process.
- Inspect a sample of supplier-reported performance metrics, and identify where performance objectives have not consistently been attained.
- Determine if management has identified and assessed the performance failures and if corrective action and a process for ongoing monitoring has been implemented.
- For a sample of service suppliers, obtain the supplier's reported performance metrics, and review them for deviations from agreed-upon performance objectives.
- Determine if supplier management is aware of the deviation and the reasonableness of actions taken (e.g., establishment of action plan, service fee penalties for non-performance).

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 Objective	Value Drivers	Risk Drivers
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.	• Efficient resource management by avoiding overhead costs • Optimised system performance achieved through internal benchmarking • Prediction of future performance and capacity requirements • Ability to benchmark capacity amongst areas of the organisation and externally to identify improvements	• Unexpected incidents due to lack of capacity • System availability faults due to a missing proactive resource capacity and performance planning • Failure to meet business requirements due to outdated performance and capacity plans

Test the Control Design

- Enquire whether and confirm that a process or framework for developing, reviewing and adjusting a performance and capacity plan is defined.
- Enquire through interviews with key staff members involved in the development of the performance and capacity plan whether the appropriate elements (e.g., customer requirements, business requirements, cost, application performance requirements, scalability requirements) have been considered during development of the capacity plan.
- Enquire whether and confirm that the performance and capacity plan has been developed and is maintained.
- Inspect supporting documents to verify stakeholder involvement and to ensure that the plan has been recorded and is up to date.

DS3 Manage Performance and Capacity (cont.)

Control Objective	Value Drivers	Risk Drivers
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.	• Efficient and effective IT resource management • Improved performance and capacity planning • System performance optimised by proactive performance and capacity planning	• Business disruptions • SLAs not met • Business requirements not met • Under- or over-commitments on service delivery due to unknown capacity measures

Test the Control Design

- Enquire whether and confirm that system monitoring software has been implemented on the appropriate IT resources based on factors such as:
  - Business criticality of the IT resource
  - Requirements identified in the SLA
  - Likelihood or historical tendency of the IT resource to experience performance or capacity issues
  - Operational/financial/regulatory impact from performance or capacity issues
- Determine whether thresholds have been established and implemented on IT resources based on business requirements and SLAs. Examples of thresholds include:
  - The call centre adding additional trunk capacity on inbound toll free lines when trunks are 80 percent busy
  - Servers adding additional disk space when hard drives reach a specific capacity level
- Determine how incidents of inadequate performance are identified and tracked.
- Obtain trouble tickets and trace identified transactions through the system to determine if proper follow-up has occurred.
- Enquire of key staff members responsible for the organisation's delivery with SLAs to determine how they monitor, track and report on IT resource capacity and performance metrics.
- Review operational reports that are provided to key stakeholders.

DS3 Manage Performance and Capacity (cont.)

Control Objective	Value Drivers	Risk Drivers
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.	• Optimised usage of IT resources • Forecasted business demands on the IT infrastructure • Improved performance and capacity planning	• Leveraged service levels not provided to the business • System unavailability due to failing IT resources • High processing loads not met by the systems

Test the Control Design

- Confirm (by interviewing key staff members and inspecting process documentation and reports) the use of appropriate tools, techniques and processes to perform the following:
  - Measuring actual performance and capacity
  - Performing reviews of capacity usage, bandwidth (e.g., network and trunk utilisation reports) and performance reports
  - Comparing actual vs. forecasted demand of resources
  - Involving management in reviewing forecasting reports and discussing any variances
- Inspect documents that measure actual IT resource performance with expected capacity and performance.
- Determine how variances in actuals vs. baselines/models are used in revising forecasting models, and ensure that an analysis is periodically performed in a timely manner.
- Enquire of key staff members whether they are knowledgeable of the capacity planning process and how they are made aware of new business requirements that may require changes to applications, servers or other IT resources.
- Confirm with key staff members the process for co-ordinating the planning and acquisition of IT resources when dictated by forecasting models.
- Review a representative sample of SLAs and OLAs and the capacity plan for regular adjustments necessitated by the reviews of forecasted performance and capacity usage.

DS3 Manage Performance and Capacity (cont.)

Control Objective	Value Drivers	Risk Drivers
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.	• Effective IT resource utilisation • Service levels meeting the business requirements • Effective IT resource availability management	• System unavailability due to failing IT resources • Inability to predict availability and serviceability of IT services • Unexpected outages of IT services

Test the Control Design

- Enquire of key staff members about the process to obtain, review and implement vendor requirements, and confirm that the current capacity and performance capabilities have incorporated the vendor requirements.
- Inspect vendor documentation to validate that it specifies vendor requirements and recommendations for minimal and optimal IT resource capacity and performance.
- Enquire of management for known performance and capacity gaps.
- Compare this information with the results of current performance monitoring and forecasted capacity requirements.
- Verify whether there is a prioritised list of activities to be supported by the IT applications.
- Verify that the capacity plan has been updated with corrective actions.
- Verify whether the planning processes (PO2-PO3) have received the updated capacity plan for their input.
- Verify whether corrective actions have been duly processed by the change management process.
- Enquire of key staff members about the process to correct performance and capacity issues.
- Obtain trouble tickets and trace identified transactions (i.e., adding additional systems, shifting processing workloads to alternative servers) through the system to determine if proper corrective action has been performed.
- Inspect the escalation procedures related to IT resource performance issues.
- Enquire of key staff members whether emergency problems have occurred in the recent past, verify compliance to the procedure and determine whether it was effective.

DS3 Manage Performance and Capacity (cont.)

Control Objective	Value Drivers	Risk Drivers
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.	• Issues identified impacting effective service delivery • Baselined service levels identifying gaps in expectations • Increased IT resource utilisation for improved service delivery	• Lack of performance monitoring • Service failing to meet the expected quality • Deviations not identified in a timely manner, thus impacting the service quality

Test the Control Design

- Enquire through interviews with key staff members involved whether a process for gathering data (e.g., IT resource requirements, capacity, availability, utilisation, recommendations on resource allocation, prioritisation) to aid management has been established.
- Enquire through interviews with management whether monitoring and reporting activities are formalised and integrated.
- Trace feedback of monitoring and reporting results to capacity planning and performance activities.
- Enquire whether and confirm that capacity reports are fed into the strategic IT planning and budgeting process.

Take the following steps to test the outcome of the control objectives:
- Inspect IT resource performance and capacity planning documentation to identify if the planning process:
  - Requires the inclusion of key metrics to be derived from SLAs
  - Factors in business requirements, technical requirements and cost considerations
  - Includes models of current and forecasted performance and capacity
  - Involves the documentation of approvals from stakeholders
  - Involves the continuous monitoring and reporting of IT
- Inspect IT resource uptime and utilisation reports to determine whether current IT capabilities are adequate.
- Enquire whether and confirm that benchmarking studies are performed to identify how competitors in similar industries are addressing performance and capacity forecasting.
- Inspect documentation that provides IT resource availability information on areas such as:
  - Storage requirements and current capacity
  - Fault tolerance and redundancy
  - Reallocation of IT resources to address availability, capacity and performance issues
- Enquire of key staff members on whether monitoring processes exist and are reported on to manage the performance, capacity and allocation of IT resources.
- Inspect performance reporting documents to verify that appropriate information is provided to management on a periodic basis.
- Verify that performance and availability plans are used in budgeting processes and for improvements to the information architecture.

Take the following steps to document the impact of the control weaknesses:
- Inspect incident reports and enquire of key staff members whether any outages are consistently being caused by capacity or performance issues.
- Enquire of key staff members responsible for maintaining IT resources to determine whether they are informed of changes to business requirements and SLAs that impact capacity and performance.

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 Objective	Value Drivers	Risk Drivers
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.	• Continuous service across IT • Consistent, documented IT continuity plans • Governed services for business needs • Achieved short- and long-range objectives supporting the organisation's objectives	• Insufficient continuity practices • IT continuity services not managed properly • Increased dependency on key individuals

Test the Control Design

- Enquire whether and confirm that an enterprisewide business continuity management process is designed and approved by executive-level management.
- Inspect the current business impact analysis and determine whether continuity planning has resulted in clear positioning of required resources to recover the business operations during a disruption.
- Inspect the business continuity framework to confirm that it includes all the elements required to resume business processing in the event of a business interruption (consider accountability, communication, escalation plan, recovery strategies, IT and business service levels, and emergency procedures).

DS4 Ensure Continuous Service (cont.)

Control Objective	Value Drivers	Risk Drivers
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.	• Continuous service across IT, addressing the requirements for critical IT resources • Defined and documented guidelines, roles and responsibilities • Achieved short- and long-range objectives supporting the organisation's objectives	• Failure to recover IT systems and services in a timely manner • Failure of alternative decision-making processes • Lack of required recovery resources • Failed communication to internal and external stakeholders

Test the Control Design

- Confirm that business continuity plans exist for all key business functions and processes.
- Review an appropriate sample of business continuity plans and confirm that each plan:
  - Is designed to establish the resilience, alternative processing and recovery capability in line with service commitments and availability targets
  - Defines roles and responsibilities
  - Includes communication processes
  - Defines the minimum acceptable recovery configuration
- Obtain the overall testing strategy for business continuity plans and evidence that tests are being executed with the agreed-upon frequency.
- Review the outcome of testing, and ensure that resulting actions are followed up.

DS4 Ensure Continuous Service (cont.)

Control Objective	Value Drivers	Risk Drivers
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.	• Cost management for continuity • Effective management of critical IT resources • Prioritised recovery management	• Unavailability of critical IT resources • Increased costs for continuity management • Prioritisation of services recovery not based on business needs

Test the Control Design

- Obtain a list of business functions with their respective business criticality, and ensure that continuity plans exist for the most critical business functions, supporting processes and resources.
- Review the plans to ensure that they are designed (and tested) to meet business objectives and legal and regulatory requirements.
- Determine how consistency between plans is ensured.

Control Objective	Value Drivers	Risk Drivers
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.	• Appropriate IT continuity plans supporting the organisation's objectives • Change control procedures for IT continuity plans • Familiarity of IT continuity plans for appropriate individuals	• Inappropriate recovery plans • Plans failing to reflect changes to business needs and technology • Lack of change control procedures

Test the Control Design

- Enquire whether and confirm that all copies of the IT continuity plan are updated with revisions and are stored on- and offsite
- Enquire whether and confirm that all critical changes to IT resources are communicated to the continuity manager for update of the IT continuity plan.
- Enquire whether and confirm that changes to the continuity plan are made at intervals appropriate for the triggers and follow accepted change control procedures.

DS4 Ensure Continuous Service (cont.)

Control Objective	Value Drivers	Risk Drivers
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.	• Effective recovery of IT systems • Staff experienced in the recovery processes for IT systems • Upgraded plans overcoming shortcomings in the restoration of systems	• Shortcomings in recovery plans • Outdated recovery plans that do not reflect the current architecture • Inappropriate recovery steps and processes • Inability to effectively recover should real disaster occur

Test the Control Design

- Enquire whether and confirm that IT continuity tests are scheduled and completed on a regular basis after changes to the IT infrastructure or business and related applications.
- Ensure that new components and updates are included in the schedule.
- Enquire whether and confirm that a detailed test schedule has been created and includes testing details and event chronology to ensure a logical and real sequence of occurring interruptions.
- Enquire whether and confirm that a test task force has been established, and the members are not key personnel defined in the plan and the reporting is appropriate.
- Enquire through interviews with key staff members whether debriefing events occur and, within these events, whether failures are analysed and solutions are developed.
- Enquire through interviews with key staff members whether alternative means are evaluated when testing is not feasible.
- Enquire whether and confirm that success or failure of the test is measured and reported and the consequential change is made to the IT continuity plan.
- Review results and evaluate how the results are reviewed to determine operating effectiveness.

Control Objective	Value Drivers	Risk Drivers
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.	• Staff experienced in the recovery processes for IT systems • Staff trained in the recovery processes • Scheduled training for all responsible staff members • Training plans updated to reflect the results of the contingency tests	• Outdated training schedules • Failure to recover as expected due to inadequate or outdated training

Test the Control Design

- Enquire through interviews with key staff members whether regular training is performed.
- Enquire whether and confirm that training needs and schedules are assessed and updated regularly.
- Review schedules and training material to determine operating effectiveness.
- Enquire through interviews with key staff members whether IT continuity awareness programmes are being performed on all levels.

DS4 Ensure Continuous Service (cont.)

Control Objective	Value Drivers	Risk Drivers
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.	• Staff experienced in the recovery processes for IT systems • Staff trained in the recovery processes • Plans available and accessible to all affected parties	• Confidential information in the plans compromised • Plans not accessible to all required parties • Upgrades of the plan not performed in a timely manner due to uncontrolled distribution strategies

Test the Control Design

- Enquire whether and confirm that a distribution list for the IT continuity plan is created, defined and maintained. Review whether the need-to-know principles have been maintained during development of the list.
- Obtain the distribution procedure from management.
- Evaluate the procedure and verify compliance.
- Enquire whether and confirm that all digital and physical copies of the plan are protected in an appropriate manner and that the documents are accessible only by authorised personnel.

Control Objective	Value Drivers	Risk Drivers
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.	• Minimised recovery times • Minimised recovery costs • Prioritised recovery of business-critical tasks	• Shortcomings in recovery plans • Inappropriate recovery steps and processes • Failure to recover business-critical systems and services in a timely manner

Test the Control Design

- Obtain a copy of the incident handling procedure, and ensure that it includes steps for damage assessment as well as formal decision points and thresholds to activate continuity plans.
- Review IT recovery plans, and confirm that they meet business requirements.

DS4 Ensure Continuous Service (cont.)

Control Objective	Value Drivers	Risk Drivers
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.	• Availability of backup data in the event of physical destruction of hardware • Offsite data consistently managed throughout the organisation • Appropriate protection of offsite storage	• Unavailability of backup data and media due to missing documentation in offsite storage • Loss of data due to disaster • Accidental destruction of backup data • Inability to locate backup tapes when needed

Test the Control Design

- Enquire whether and confirm that data are protected when they are taken offsite, whilst they are in transport and when they are at the storage location.
- Enquire whether and confirm that the backup facilities are not subject to the same risks as the primary site.
- Enquire whether and confirm that regular testing is performed to ensure the quality of the backups and media.
- Review testing procedures to determine operating effectiveness.
- Verify that the backup media contain all information required by the IT continuity plan, e.g., by comparing the contents of the backups and/or the restored systems with the operational systems.
- Enquire whether and confirm that sufficient recovery instructions and labelling exist.
- Enquire whether and confirm that an inventory of backups and media exists, and verify its correctness.

Control Objective	Value Drivers	Risk Drivers
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.	• Updated recovery plans • Objectives met by the recovery plans • Adequate resumption plans according to business needs	• Inappropriate recovery plans • Recovery plans failing to meet business needs • Objectives not met by the recovery plans

Test the Control Design

- Enquire whether and confirm that the shortcomings of the plan have been highlighted and post-recovery meetings discussing opportunities for improvement are performed.
- Review plans, policies and procedures to determine operating effectiveness.

Take the following steps to test the outcome of the control objectives:
- Determine the management level for establishing the continuity framework to support enterprisewide business processing recovery processes.
- Determine the components defined to address the IT continuity accountabilities and responsibilities for supporting the business strategy in response to a business disruption.
- Assess the IT continuity plans for recovery strategies and required service levels to meet the business processing objectives.
- Determine the effectiveness of the communications plan created to ensure the safety of all affected parties and co-ordination with public authorities.
- Assess the guidelines, roles and responsibilities achieving recovery of short- and long-range business processing requirements.
- Assess whether IT continuity planning training is provided on a periodic basis.

Take the following steps to document the impact of the control weaknesses:
- Assess whether the IT continuity services sufficiently support achieving business processing services to meet short- and long-range organisation objectives.
- Assess the framework to determine whether the planning invokes dependencies on key individuals rather than prioritisation of recovery strategies.
- Assess the impact on business processing in the event IT systems are not recovered in a timely manner without an alternative decision-making process.
- Determine the business impact required if recovery resources are not available and there is no ability to communicate with internal and external stakeholders.
- Enquire of management whether IT disruptions were prolonged as a result of untrained staff members who did not follow IT continuity planning procedures.

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 responsibilities, 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.

Control Objective	Value Drivers	Risk Drivers
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.	• Critical IT assets protected • IT security strategy supporting business needs • IT security strategy aligned with the overall business plan • Appropriately implemented and maintained security practices consistent with applicable laws and regulations	• Lack of IT security governance • Misaligned IT and business objectives • Unprotected data and information assets

Test the Control Design

- Determine if a security steering committee exists, with representation from key functional areas, including internal audit, HR, operations, IT security and legal.
- Determine if a process exists to prioritise proposed security initiatives, including required levels of policies, standards and procedures.
- Enquire whether and confirm that an information security charter exists.
- Review and analyse the charter to verify that it refers to the organisational risk appetite relative to information security and that the charter clearly includes:
  - Scope and objectives of the security management function
  - Responsibilities of the security management function
  - Compliance and risk drivers
- Enquire whether and confirm that the information security policy covers the responsibilities of board, executive management, line management, staff members and all users of the enterprise IT infrastructure and that it refers to detailed security standards and procedures.
- Enquire whether and confirm that a detailed security policy, standards and procedures exist. Examples of policies, standards and procedures include:
  - Security compliance policy
  - Management risk acceptance (security non-compliance acknowledgement)
  - External communications security policy
  - Firewall policy
  - E-mail security policy
  - An agreement to comply with IS policies
  - Laptop/desktop computer security policy
  - Internet usage policy
- Enquire whether and confirm that an adequate organisational structure and reporting line for information security exist, and assess if the security management and administration functions have sufficient authority.
- Enquire whether and confirm that a security management reporting mechanism exists that informs the board, business and IT management of the status of information security.

DS5 Ensure Systems Security (cont.)

Control Objective	Value Drivers	Risk Drivers
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.	• The IT security plan satisfying business requirements and covering all risks to which the business is exposed • Investments in IT security managed in a consistent manner to enable the security plan • Security policies and procedures communicated to stakeholders and users • Users aware of the IT security plan	• IT security plan not aligned with business requirements • IT security plan not cost effective • Business exposed to threats not covered in the strategy • Gaps between planned and implemented IT security measures • Users not aware of the IT security plan • Security measures compromised by stakeholders and users

Test the Control Design

- Determine the effectiveness of the collection and integration of information security requirements into an overall IT security plan that is responsive to the changing needs of the organisation.
- Verify that the IT security plan considers IT tactical plans (PO1), data classification (PO2), technology standards (PO3), security and control policies (PO6), risk management (PO9), and external compliance requirements (ME3).
- Determine if a process exists to periodically update the IT security plan, and if the process requires appropriate levels of management review and approval of changes.
- Determine if enterprise information security baselines for all major platforms are commensurate with the overall IT security plan, if the baselines have been recorded in the configuration baseline (DS9) central repository, and if a process exists to periodically update the baselines based on changes in the plan.
- Determine if the IT security plan includes the following:
  – A complete set of security policies and standards in line with the established information security policy framework
  – Procedures to implement and enforce the policies and standards
  – Roles and responsibilities
  – Staffing requirements
  – Security awareness and training
  – Enforcement practices
  – Investments in required security resources
- Determine if a process exists to integrate information security requirements and implementation advice from the IT security plan into other processes, including the development of SLAs and OLAs (DS1-DS2), automated solution requirements (AI1), application software (AI2), and IT infrastructure components (AI3).

DS5 Ensure Systems Security (cont.)

Control Objective	Value Drivers	Risk Drivers
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.	• Effective implementation of changes • Proper investigation of improper access activity • Secure communication ensuring approved business transactions	• Unauthorised changes to hardware and software • Access management failing business requirements and compromising the security of business-critical systems • Unspecified security requirements for all systems • Segregation-of-duty violations • Compromised system information

Test the Control Design

- Determine if security practices require users and system processes to be uniquely identifiable and systems to be configured to enforce authentication before access is granted.
- If predetermined and preapproved roles are utilised to grant access, determine if the roles clearly delineate responsibilities based on least privileges and ensure that the establishment and modification of roles are approved by process owner management.
- Determine if access provisioning and authentication control mechanisms are utilised for controlling logical access across all users, system processes and IT resources, for in-house and remotely managed users, processes and systems.

Control Objective	Value Drivers	Risk Drivers
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.	• Consistently managed and administered user accounts • Rules and regulations for all kinds of users • Timely discovery of security incidents • Protection of IT systems and confidential data from unauthorised users	• Security breaches • Users failing to comply with security policy • Incidents not solved in a timely manner • Failure to terminate unused accounts in a timely manner, thus impacting corporate security

Test the Control Design

- Determine if procedures exist to periodically assess and recertify system and application access and authorities.
- Determine if access control procedures exist to control and manage system and application rights and privileges according to the organisation's security policies and compliance and regulatory requirements.
- Determine if systems, applications and data have been classified by levels of importance and risk, and if process owners have been identified and assigned.
- Determine if user provisioning policies, standards and procedures extend to all system users and processes, including vendors, service providers and business partners.

DS5 Ensure Systems Security (cont.)

Control Objective	Value Drivers	Risk Drivers
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.	• Staff experienced in security testing and monitoring of IT systems • Regularly reviewed security level • Deviations from business requirements highlighted • Security breaches detected proactively	• Misuse of users' accounts, compromising organisational security • Undetected security breaches • Unreliable security logs

Test the Control Design

- Enquire whether and confirm that an inventory of all network devices, services and applications exists and that each component has been assigned a security risk rating.
- Determine if security baselines exist for all IT utilised by the organisation.
- Determine if all organisation-critical, higher-risk network assets are routinely monitored for security events.
- Determine if the IT security management function has been integrated within the organisation's project management initiatives to ensure that security is considered in development, design and testing requirements, to minimise the risk of new or existing systems introducing security vulnerabilities.

DS5 Ensure Systems Security (cont.)

Control Objective	Value Drivers	Risk Drivers
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.	• Proactive security incident detection • Reporting of security breaches on a defined and documented level • Identified ways of communication for security incidents	• Undetected security breaches • Lack of information for performing counterattacks • Missing classification of security breaches

Test the Control Design

- Determine if a computer emergency response team (CERT) exists to recognise and effectively manage security emergencies. The following areas should exist as part of an effective CERT process:
  - Incident handling—General and specific procedures and other requirements to ensure effective handling of incidents and reported vulnerabilities
  - Vendor relations—The role and responsibilities of vendors in incident prevention and follow-up, software flaw correction, and other areas
  - Communications—Requirements, implementation and operation of emergency and routine communications channels amongst key members of management
  - Legal and criminal investigative issues—Issues driven by legal considerations and the requirements or constraints resulting from the involvement of criminal investigative organisations during an incident
  - Constituency relations—Response centre support services and methods of interaction with constituents, including training and awareness, configuration management, and authentication
  - Research agenda and interaction—Identification of existing research activities and requirements and rationale for needed research relating to response centre activities
  - Model of the threat—Development of a basic model that characterises potential threats and risks to help focus risk reduction activities and progress in those activities
  - External issues—Factors that are outside the direct control of the company (e.g., legislation, policy, procedural requirements) but that could affect the operation and effectiveness of the company's activities
- Determine if the security incident management process appropriately interfaces with key organisation functions, including the help desk, external service providers and network management.
- Evaluate if the security incident management process includes the following key elements:
  - Event detection
  - Correlation of events and evaluation of threat/incident
  - Resolution of threat, or creation and escalation work order
  - Criteria for initiating the organisation's CERT process
  - Verification and required levels of documentation of the resolution
  - Post-remediation analysis
  - Work order/incident closure

DS5 Ensure Systems Security (cont.)

Control Objective	Value Drivers	Risk Drivers
DS5.7 Protection of Security Technology Make security-related technology resistant to tampering, and do not disclose security documentation unnecessarily.	• Corporate security technology protected • Reliable information secured • Corporate assets protected	• Exposure of information • Breach of trust with other organisations • Violations of legal and regulatory requirements

Test the Control Design

- Enquire whether and confirm that policies and procedures have been established to address security breach consequences (specifically to address controls to configuration management, application access, data security and physical security requirements).
- Inspect the control records granting and approving access and logging unsuccessful attempts, lockouts, authorised access to sensitive files and/or data, and physical access to facilities.
- Enquire whether and confirm that the security design features facilitate password rules (e.g., maximum length, characters, expiration, reuse).
- Enquire whether and confirm that the control requires annual management reviews of security features for physical and logical access to files and data.
- Verify that access is authorised and appropriately approved.
- Inspect security reports generated from system tools preventing network penetration vulnerability attacks.

DS5 Ensure Systems Security (cont.)

Control Objective	Value Drivers	Risk Drivers
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.	• Defined and documented key management • Keys handled in a secure manner • Secure communication	• Keys misused by unauthorised parties • Registration of non-verified users, thus compromising system security • Unauthorised access to cryptographic keys

Test the Control Design

- Determine if a defined key life cycle management process exists. The process should include:
  - Minimum key sizes required for the generation of strong keys
  - Use of required key generation algorithms
  - Identification of required standards for the generation of keys
  - Purposes for which keys should be used and restricted
  - Allowable usage periods or active lifetimes for keys
  - Acceptable methods of key distribution
  - Key backup, archival and destruction
- Assess if controls over private keys exist to enforce their confidentiality and integrity. Consideration should be given to the following:
  - Storage of private signing keys within secure cryptographic devices (e.g., FIPS 140-1, ISO 15782-1, ANSI X9.66)
  - Private keys not exported from a secure cryptographic module
  - Private keys backed up, stored and recovered only by authorised personnel using dual control in a physically secured environment
- Enquire whether and confirm that the organisation has implemented information classification and associated protective controls for information that account for the organisation's needs for sharing or restricting information and the organisational impacts associated with such needs.
- Determine if procedures are defined to ensure that information labelling and handling is performed in accordance with the organisation's information classification scheme.

DS5 Ensure Systems Security (cont.)

Control Objective	Value Drivers	Risk Drivers
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).	• System security ensured by proactive malware protection • Ensured system integrity • Timely detection of security threats	• Exposure of information • Violations of legal and regulatory requirements • Systems and data that are prone to virus attacks • Ineffective countermeasures

Test the Control Design

- Enquire whether and confirm that a malicious software prevention policy is established, documented and communicated throughout the organisation.
- Ensure that automated controls have been implemented to provide virus protection and that violations are appropriately communicated.
- Enquire of key staff members whether they are aware of the malicious software prevention policy and their responsibility for ensuring compliance.
- From a sample of user workstations, observe whether a virus protection tool has been installed and includes virus definition files and the last time the definitions were updated.
- Enquire whether and confirm that the protection software is centrally distributed (version and patch-level) using a centralised configuration and change management process.
- Review the distribution process to determine the operating effectiveness.
- Enquire whether and confirm that information on new potential threats is regularly reviewed and evaluated and, as necessary, manually updated to the virus definition files.
- Review the review and evaluation process to determine operating effectiveness.
- Enquire whether and confirm that incoming e-mail is filtered appropriately against unsolicited information.
- Review the filtering process to determine operating effectiveness, or review the automated process established for filtering purposes.

DS5 Ensure Systems Security (cont.)

Control Objective	Value Drivers	Risk Drivers
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.	• Corporate security technology protected • Reliable information secured • Corporate assets protected • Network security managed in a consistent manner	• Failure of firewall rules to reflect the organisation's security policy • Undetected unauthorised modifications to firewall rules • Compromised overall security architecture • Security breaches not detected in a timely manner

Test the Control Design

- Enquire whether and confirm that a network security policy (e.g., provided services, allowed traffic, types of connections permitted) has been established and is maintained.
- Enquire whether and confirm that procedures and guidelines for administering all critical networking components (e.g., core routers, DMZ, VPN switches) are established and updated regularly by the key administration personnel, and changes to the documentation are tracked in the document history.

Control Objective	Value Drivers	Risk Drivers
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.	• Trusted ways of communications • Reliable information exchange • System and data integrity safeguarded	• Sensitive information exposed • Inadequate physical security measures • Unauthorised external connections to remote sites • Disclosure of corporate assets and sensitive information accessible for unauthorised parties

Test the Control Design

- Enquire whether and confirm that data transmissions outside the organisation require encrypted format prior to transmission.
- Enquire whether and confirm that corporate data are classified according to exposure level and classification scheme (e.g., confidential, sensitive).
- Enquire whether and confirm that sensitive data processing is controlled through application controls that validate the transaction prior to transmission.
- Review that the application logs or halts processing for invalid or incomplete transactions.

Take the following steps to test the outcome of the control objectives:

- Through inquiry and observation, determine if the security management function effectively interacts with key enterprise functions, including areas such as risk management, compliance and audit.
- Review the process for identifying and responding to security incidents, selecting a sample of recorded incidents. Through inquiry and review of supporting documentation, determine whether appropriate management action has been taken to resolve the incident.
- Select a sample of employees and determine if computer usage and confidentiality (non-disclosure) agreements have been signed as part of their initial terms and conditions of employment.
- Review the IT security strategy, plans, policies and procedures to determine their relevance to the organisation's current IT landscape, and determine when they were last reviewed and updated.
- Review the IT security strategy, plans, policies and procedures, and verify that they reflect the data classification.
- Interview stakeholders and users on their knowledge of the IT security strategy, plans, policies and procedures, and determine if stakeholders and users find them to be relevant to risks and organisational practices.
- Ask executive management about any recent or planned changes to the organisation (e.g., business unit acquisitions/dispositions, new systems, changes in regulatory environment), and determine if the IT security plan is properly aligned.
- Determine if security processes have been implemented to uniquely identify and control the actions of all users and processes through review of system (development, test and production systems) and application accounts, job queues and services, and security software mode settings.
- Through a sample of access control lists (ACLs), determine whether the security provisioning process appropriately considers the following:
  - Sensitivity of the information and applications involved (data classification)
  - Policies for information protection and dissemination (legal, regulatory and contractual requirements)
  - The 'need-to-have' of the function
  - Standard user access profiles for common job roles in the organisation
  - The need for segregation for the access rights involved
  - Data owner and management's authorisation for access
  - The documentation of identity and access rights in a central repository
  - Creation, communication and change of initial passwords
- Through inquiry and review of sampled ACLs, determine if a process exists for resolving access provisioning requests that are not commensurate with established security authentication practices and roles.
- Determine if a risk assessment process was utilised to identify possible segregation of duties and if an escalation process was utilised to obtain added levels of management authorisation.
- Determine if authentication and authorisation mechanisms exist to enforce access rights according to the sensitivity and criticality of information (e.g., password, token, digital signature).
- Determine if trust relationships enforce comparable security levels and maintain user and process identities.
- Select a sample of user and system accounts and a sample ACL to determine existence of the following:
  - Clearly defined requested role and/or privileges
  - Business justification for assignment
  - Data owner and management authorisation
  - Business/risk justification and management approval for non-standard requests
  - Access requested commensurate with job function/role and required segregation of duties
  - Documentation evidencing adherence to and completion of the provisioning process
- Obtain from HR a sample of employee transfers and terminations and, through review of system account profiles and/or ACLs, determine if access has been appropriately altered and/or revoked in a timely manner.
- Select a sample of critical network devices and system services, and determine if access control mechanisms have been routinely evaluated and tested to confirm their operational effectiveness.
- Select a sample of critical network devices and system services, and determine if they have been routinely monitored for existence of security incidents.
- Sample security baselines and determine if they are appropriately aligned to the organisation's risk profile and levels of accepted risk and if they take into account common risks and vulnerabilities (i.e., conform to leading practices).
- Select a sample of IT devices and determine their compliance with established security baselines. For deviations from baselines, determine if a risk assessment was performed and if management approved the deviation from the baseline.
- Determine if a security review process has been integrated into the organisation's acquisition and implementation processes (AI) and delivery and support processes (DS), requiring security management's involvement and approval of any IT changes that would impact the design or operation systems security. The review process should consider:
  - Overall technology architecture
  - Database access and security design
  - Protocol, port and socket usage
  - Required services

  – User remote access and modem requirements
  – Server-to-server authentication and encryption
  – Scalability, availability and redundancy
  – Session management and cookie usage
  – Administrative capabilities
  – User ID and password management
  – Audit trails and logging/reporting
- Determine if security audit trails capture user identification (ID), type of event, date and time, success or failure indication, origination of event, and the identity or the name of the affected object. Logged events should include accesses to sensitive data, actions by administrative and privileged accounts, initialisation of audit logs, and modification of system-level objects.
- Inspect and review documents supporting the recording, analysis and resolution of potential security incidents, and perform the following steps:
  – Understand the methods used to categorise incidents and identify actionable threats.
  – Identify specific logged security incidents, and inquire as to the nature and disposition of the incident.
- Inspect documentation evidencing the process used to match the organisation's network device inventory to published vulnerabilities for the purpose of verifying that all devices are at current release and security patch levels.
- Determine if formal management responsibilities and procedures exist throughout the key management life cycle, including changes to encryption equipment, software and operating procedures.
- For a sample of new keys, determine if key pairs have been generated in accordance with industry standards and compliance or regulatory requirements (e.g., ISO 15782-1, FIPS 140-1, ANSI X9.66) and if documentation evidences the existence of split-knowledge and dual-control keys (requiring two or three people, each knowing only his/her part of the key, to reconstruct the whole key).
- For a sample of expired keys, determine if documentation exists evidencing the complete destruction of keys at the end of the key-pair life cycle.
- Review maintenance records evidencing that cryptographic hardware is routinely tested.
- Obtain a list of individuals who have access to cryptographic hardware, software and keys, and determine if access is limited to properly authorised individuals responsible for the creation and injection of keys.
- Determine if key custodians formally acknowledge, understand and accept their key custodian responsibilities.
- Determine if encryption keys are generated, stored and used in a manner such that the keys and their components are known only to authorised custodians.
- For keys received from third-party vendors, determine if they are sent in separate parts by different carriers on different dates, and if each part of the key is stored in a separate safe, for which the combination is known by a separate key officer.
- Assess the system security features to evaluate whether proactive controls have been established to protect from malicious security attacks.
- Assess whether the data/system protection software is centrally distributed throughout the network environment.
- Assess the control features for filtering incoming traffic against unsolicited information.
- Select a sample of critical network devices, and confirm that the devices are properly secured with special mechanisms and tools (e.g., authentication for device management, secure communications, strong authentication mechanisms) and that active monitoring and pattern recognition are in place to protect devices from attack.
- Select a sample of network devices, and determine if the devices have been configured with minimal features enabled (e.g., features that are necessary for functionality and hardened for security applications); all unnecessary services, functionalities and interfaces have been removed; and all relevant security patches and major updates are applied to the system in a timely manner before going to production.
- Select a sample of new network devices or changes to existing network devices and determine that the organisation's Acquire and Implement (AI) process controls and Deliver and Support (DS) process controls have been followed.
- Select a sample of firewall devices, and review ACLs for the following:
  – Access rules effectively segregating trusted and non-trusted network segments
  – Documentation evidencing the business purpose and management's approval of rules
  – Configurations following management-approved baselines
  – Devices that are current on version and patch release levels
- Determine if encryption is utilised for all non-console administrative access, such as SSH, VPN or SSL/TLS.
- Assess whether automated controls safeguard the data and systems, such that data are transmitted through reliable sources.
- Determine if user management periodically reviews user profiles and access rights to ensure the adequacy of access rights and requirements for segregation of duties.
- Verify that direct access to data is prevented or, where required, controlled and documented accordingly.
- Verify that the quality requirements for passwords are defined and enforced by systems.

Take the following steps to document the impact of the control weaknesses:

- Determine the level of security consciousness within the organisation by reviewing functional and operational documentation for the existence of security considerations (e.g., involvement of the security management function within the SDLC).
- Benchmark the information security organisation (e.g., size, lines of reporting) against similar organisations, and benchmark formalised policies, standards and procedures to international standards/recognised industry best practices.
- Determine if the security management function is commensurate with the size and complexity of the IT landscape. Consider the following:
  – Size, complexity and diversity of the IT landscape
  – Use of security administration tools and technology
  – Alignment of security management to business lines (e.g., do organisation segments have competing security functions?)
  – Skills and training of security management personnel
- Determine if members of executive management communicate the importance and their support of the security management organisation. Consideration should be given to executive management or security steering committee approval of formalised security policies.
- Determine the existence of a management-approved security charter and policies, standards and procedures that address logical security for all relevant aspects of the organisation's IT landscape.
- Determine if the IT security plan has adequately considered the security profile of the organisation, including any regulatory and compliance requirements.
- Assess the ability of the security management organisation to execute and monitor compliance with the plan. Consideration should be given to the size of the organisation, use of security assessment and administration technology and tools, and required experience levels and ongoing training received by security personnel.
- Select policy, standards and procedural documentation from various financial, operational and compliance areas within the organisation, and determine if key provisions of the IT security plan have been appropriately reflected in the documentation.
- Determine if a security review process has been integrated into the organisation's AI and DS processes, requiring security management's involvement and approval of any IT changes that would impact the design or operation systems security.
- Determine if the organisation's AI processes and controls are supported by segregated development, test and assurance, and production environments.
- Identify the existence and reasonableness of anonymous and group accounts (e.g., nobody, web user, everybody), remote processes and started tasks. Consideration should be given to the nature and scope of transaction authorities, the risk of possible escalation of privileges, the process origin (e.g., trusted, non-trusted), or if a security design review was performed for system and application-initiated jobs and processes.
- Determine if security software, applications and supporting systems software has been configured to enforce user authentication or propagate user and process identities. Determine if default accounts exist to authenticate anonymous users or processes.
- Determine sources of non-trusted access (e.g., business partners, vendors), and determine how access has been assigned to provide uniquely identifiable account holders and appropriate protection of information.
- Through the use of audit software tools or scripts, identify the existence of inactive or unused accounts and determine the existence of a business justification.
- Identify active vendor or contractor accounts, and determine if access is commensurate with the terms and duration of the contract.
- Determine if vendor-supplied accounts have been appropriately safeguarded (e.g., default passwords changed, accounts revoked).
- Assess the reasonableness of the nature and frequency of verification and vulnerability assessment processes utilised, considering the organisation's risk profile, size, complexity and diversity.
- Determine if security scripts and tools are utilised to test the existence of common vulnerabilities, the effectiveness of security mechanisms and the effectiveness of user access administration processes (e.g., existence of inactive or never used accounts, terminated user accounts, accounts without passwords or forced password changes).
- Identify and select a sample of organisation-critical network devices (hardware and application systems) and at-risk perimeter network devices. Determine the existence of security sensors or use of host logging to capture incidents, and ensure that security incidents are included in the daily review process.
- Obtain a sample of security-related incident work order tickets, and determine if the issue has been appropriately resolved and closed in a timely manner.
- Determine if security tool deployment appropriately addresses all principal technologies utilised by the organisation and if personnel possess the required skills to appropriately operate the security tools and technologies.
- Determine if security personnel are required to attend annual training and if security tools receive routine updates to threat and vulnerability engines and supporting database/signatures.
- Select a sample of business-critical or sensitive data, and determine if data have been secured in accordance with the organisation's encryption standards.
- Verify that the cryptographic system used to protect stored data effectively renders data unreadable, and determine if any method can be utilised to access erased data through forensic techniques.
- Determine whether the security controls have been implemented to prevent exposure from malicious attacks and vulnerabilities.

- Determine if portable code (e.g., Java, JavaScript) and downloaded binaries and executables are scanned before being allowed into the network or blocked from entering the network.
- Determine that the organisation's network documentation accurately reflects the current network environment, including wireless devices, and examine the network design to determine if security barriers are strategically placed at the network's perimeter, between the organisation's trusted internal network and non-trusted public (i.e., Internet), vendor (i.e., service organisation) or business partner (i.e., extranet) segments.
- Verify that changes to security-relevant parameters follow the organisation's change management processes and are authorised and tested accordingly.
- Confirm that sensitive information is not disclosed or exposed to unauthorised parties.

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 Objective	Value Drivers	Risk Drivers
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.	• Improved management understanding and acceptance of IT costs, thereby facilitating more effective budgeting for IT services • User management empowered with reliable, transparent information about controllable IT costs to facilitate more efficient control and prioritisation of resources • Business management able to see the total cost of each business function and, therefore, make better informed decisions	• Costs accounted for incorrectly • Investment decisions based on invalid cost information • Business users having an incorrect view of IT's cost and value contribution

Test the Control Design

- Enquire whether and confirm that a policy exists for cost allocations to departments.
- Inspect the documentation that defines the IT services and verify that the distinct IT services to which costs will be allocated have been defined and documented.
- Inspect the mapping of IT services to IT infrastructure, and determine if the mapping is appropriate by, for example, obtaining a copy of the hardware and software inventories and the listing of IT services to ensure that all infrastructure and services have been mapped.
- Confirm the sources of information used to create the mapping to determine whether the sources of information were appropriate for the mapping exercise.
- Inspect the mapping of IT services to the business process to ensure that the mapping has been done completely and appropriately. This can be accomplished by, for example, comparing the mapping to the organisational chart or lines of business.
- Enquire whether and determine if results of the mapping have been confirmed with the business process owners. Enquiries should focus on ascertaining the agreement of the business process owners with the alignment of IT services provided.
- Inspect documentation supporting the communication and agreement on mapping to determine whether agreement was achieved. Such documentation may include meeting minutes, budget documentation and SLAs.

DS6 Identify and Allocate Costs (cont.)

Control Objective	Value Drivers	Risk Drivers
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.	• More effective alignment promoted between business objectives and the cost of IT • Facilitated allocation of IT resources to competing IT projects and processes • Business units able to fully understand the total IT cost involved for delivering various business processes • The level of productivity increased and the business view and professionalism of staff within the IT organisation expanded through increased financial accountability	• Failure of the current accounting model to support equitable service chargeback • Costs recorded failing to comply with the enterprise's financial accounting policies • The business having an incorrect view of IT costs and value provided

Test the Control Design

- Obtain a copy of the cost elements defined (e.g., in an IT cost allocation model or costing system), compare them to cost elements defined for the overall organisation, and examine where differences exist.
- Identify the elements that are unique to IT, and assess the appropriateness of the cost elements defined.
- Inspect billings' cost allocation journal entries to record the allocations of IT costs and assess the appropriateness of those allocations. For example, comparisons across departments or as a percentage of department expenditures may identify misallocations or unallocated costs.
- Obtain a copy of the enterprise cost accounting system setup, and assess the treatment of IT costs through examination of IT expense registers, interdepartment billings, journal entries, etc.
- Obtain and inspect a copy of the documentation that requires budgets and forecasts to be updated on changes in cost structures, and review that documentation with business process owners and IT service leaders to determine whether the process is understood and deployed.
- Inspect documentation of the process for creating IT budgets, forecasts and actual cost reporting.
- Ensure that those processes are in alignment with the overall organisational processes, and determine whether the distribution lists and schedule for reporting on initial budgets, forecasts and actual to date are appropriate. Appropriateness of distribution includes considering all impacted business process owners, senior management, etc. Appropriateness of the schedule for distribution of reporting includes ensuring that IT is aligned with business reporting timelines.
- Assess the definitions of roles for recipients of budgets, forecasts and actual analysis to determine whether all appropriate parties have been assigned as recipients.

DS6 Identify and Allocate Costs (cont.)

Control Objective	Value Drivers	Risk Drivers
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.	• IT cost allocation transparent for all affected parties • Reliable information provided to the organisation about its total IT cost • Investment decisions relatable to current costs	• The cost model not in line with the overall accounting procedures • Gaps in identified and charged services • Service usage insufficiently measured and failing to reflect actual business usage

Test the Control Design

- Enquire whether and confirm that all chargeable items and services provided by the IT department are properly categorised and itemised and that the corresponding charges for every service are listed.
- Verify that the material is organised in line with the enterprise accounting framework.
- Confirm through interviews with major users and a review of user department complaints in chargeback invoices that the chargeback model is transparent and fair.
- Confirm through interviews with IT management that the costing and chargeback model allows for efficient resource planning.
- Select a sample resource/service, compare the total cost to income from chargeback, and analyse the gap.

Control Objective	Value Drivers	Risk Drivers
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.	• IT cost allocations continuously aligned with actual business usage of IT services • Cost allocations based on the most appropriate approach for the business and IT	• The cost model not in line with actual usage • The method used for cost allocation not appropriate for the needs of the business and IT

Test the Control Design

- Enquire whether and confirm that the cost/charge model is reviewed on a regular basis (e.g., annually or semi-annually), including the current business requirements and changes in the IT services and costs.
- Inspect the reassessed charging model documents to look for management approval and to determine operating effectiveness.
- Inspect the policy or standards requiring IT cost charge models to be performed, and ensure that there is a requirement for regular review against the enterprise model (e.g., annually or semi-annually), or that there is a process for changes to the enterprise model to be reflected in the IT models.

Take the following steps to test the outcome of the control objectives:
- Enquire whether and confirm that cost allocations to departments are acceptable and/or appropriate for the organisation.
- Enquire whether and confirm that costs are allocated to distinct IT services.
- Enquire whether and confirm that the responsibility for gathering and allocating costs has been assigned appropriately.
- Inspect documentation that defines the cost allocation approach to ascertain whether all costs are allocated reasonably. This can be accomplished by, for example, comparing cost allocations to the budget or actual expenses incurred.
- Obtain the IT budget and departmental budgets, and determine whether IT service costs exist in departmental budgets.
- Consider whether the IT budget appears to be in alignment with the business needs through examination of departmental budgets, applications supported by department, etc.
- Select a sample of costs incurred and trace those costs to ascertain that they have been appropriately allocated to the IT services.
- Extract significant costs (e.g., the top 10 percent, significant department costs), and trace those costs to ascertain that they have been appropriately allocated to the IT services.
- Extract all IT costs and stratify by type for comparison to IT service definitions.
- Confirm with IT service leaders that all infrastructure inventory is accounted for and owned by IT services provided. This can be accomplished by examining the geographic scope of IT service and the nature of applications and business services provided, and discussing those scopes with the IT service leaders or through corroborating the IT service scope discussed with the current network diagrams.
- Select a sample of IT services and inspect the allocations of IT infrastructure for completeness by considering the nature of the IT service provided and known infrastructure required for support.
- Select a sample of IT infrastructure and ensure that it is mapped or assigned to an IT service area.
- Inspect asset registries, network diagrams or other infrastructure inventories, and determine whether allocations to service owners have been made.
- Select a sample of assets from a tour of the data centre and ensure that the assets are appropriately logged in asset registries, network diagrams or other infrastructure inventories.
- Enquire whether and confirm that all defined cost elements (e.g., people, accommodations, transfers, hardware, software) have been captured.
- Inspect billings/cost allocations/journal entries to record the allocations of IT costs and assess the appropriateness of those allocations. For example, comparisons across departments, or a percentage of department expenditures, may identify misallocations or unallocated costs.
- Compare and reconcile costs allocated to departments against IT expenditures to determine whether complete and accurate allocations are occurring.
- Inspect the general ledger accounts for IT expenditures to identify high-risk accounts (e.g., accounts that are not regularly used or that have high volumes of transactions flowing through them), and review for unusual entries.
- Select a sample of invoices from the IT department, and ensure that the accounting treatment is in accordance with the enterprise's cost allocation models.
- Analyse IT cost information obtained from the general ledger accounts to determine whether accounts that are subject to auto-posted or standard journal entries are posted correctly. For example, reperform the calculation of depreciation expense on IT assets to verify that accumulated amortisation on IT is allocated appropriately to the departments based on service usage or percentage allocations.
- Confirm with business process owners that there are processes in place to prevent unauthorised changes to cost allocations and to detect/monitor changes to cost allocations.
- Inspect a sample of cost structure changes, and ensure that budgets and forecasts for the affected departments have been revised and are numerically correct.
- Inspect the change logs to identify significant changes or deployment of new systems, and determine whether those changes have had an impact on cost structures and have resulted in a subsequent change in budgets and forecasts.
- Inspect any analysis of variance amongst budgeted cost, forecasted cost and actual cost and determine whether they have been completed on a timely basis and with sufficient detail. Assess whether the analysis has been performed in alignment with organisational standards.
- Inspect distribution lists to validate whether all relevant senior management and business process owners receive analysis.
- Confirm with the business process owners how they are informed of changes to the IT service costs allocated to their departments.
- Enquire whether and confirm that inquiries due to unclear cost or pricing procedures are followed up on immediately and captured for summary analysis. Trace an inquiry through the system to determine operating effectiveness and ensure immediate follow-up.

Take the following steps to document the impact of the control weaknesses:
- Compare IT expenditure as a percentage of overall corporate expenditures, and determine if IT expenditures appear reasonable by using, for example, trend analysis over years or benchmarking against industry standards.
- Select a statistical sample of expenditures from each of the IT expense accounts and determine through statistical extrapolation the impact of misallocations and the ways in which accounts and/or departments have been affected.

- Compare and reconcile costs allocated to departments against IT expenditures to determine whether complete and accurate allocations are occurring.
- Inspect HR records to determine changes in headcount since the last cost structure change, and quantify the impact of the change on the costing models. Compare payroll registers from the prior year to the current year to assess the consistency of payroll expenditures and whether those changes have been reflected in the costing models.
- Inspect the change logs to identify significant changes or deployment of new systems, determine whether those changes have had an impact on cost structures, and quantify the impact on the costing models.
- Compare the asset registers from the prior year to the current year, identify any significant new assets, and determine whether those assets have had an impact on cost structures in terms of, for example, depreciation and amortisation. Assess whether any significant decommissioned assets have not been removed appropriately.
- Enquire of business process owners whether the lack of budget, forecast and actual cost information from IT has impacted their ability to manage costs. Determine the impact through discussion with those process owners.
- Enquire whether and confirm that all chargeable items and services provided by the IT department are itemised and that the corresponding charges for every service are listed.
- Select a statistical sample of expenditures from each of the IT expense accounts and determine through statistical extrapolation the impact of misallocations and the ways in which accounts and/or departments have been affected.

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.

Control Objective	Value Drivers	Risk Drivers
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	• Training needs for personnel identified to fulfil business requirements • A baseline for the effective use of the organisation's technology by personnel, both immediately and in the future • Establishment of training and education programmes that are relevant to the risks and opportunities the organisation faces currently and in the future • Installed application capabilities optimised to satisfy business needs	• Staff members inadequately trained to fulfil their job function • Ineffective training mechanisms • Training provided not appropriate for training need • Installed application capabilities underutilised

Test the Control Design

- Enquire whether and confirm that a plan for training and professional development of IT staff members exists.
- Obtain and inspect the curriculum for completeness (e.g., depth and breadth of coverage, frequency of classes, class schedule, complexity of class, source of training—vendor local school or trade institute).
- Obtain and inspect the training calendar.
- Obtain and review the training budget.
- Obtain a copy of test completions, scoring and attendance confirmation (e.g., online training course evidence of exams and attendance).
- Determine management's process for developing and maintaining a skill inventory.
- Obtain and review the skills inventory catalogue to determine whether the skills catalogued map to the systems deployed.
- Determine that the skills database is current and available knowledge is maintained as current.
- Inspect the training strategy to ensure that training needs are to be incorporated into users' individual performance plans.
- Inspect documentation detailing the requirement to analyse root causes, including training, from the service desk outputs.

DS7 Educate and Train Users (cont.)

Control Objective	Value Drivers	Risk Drivers
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.	• Formalised and communicated management commitment for training • Effective trainers and training programmes • Sufficient attendance and involvement in training programmes and sessions	• Inappropriate and ineffective training programmes and mechanisms selected • Outdated training materials used • Poor attendance and involvement recorded

Test the Control Design

- Review the training schedule, and confirm that it meets training needs.
- Ensure that adequate resources are available to deliver training.
- Analyse a sample of the training programmes and verify:
  - Contents vs. objectives
  - Actual vs. planned attendance
  - Attendee satisfaction
  - Application of feedback received

Control Objective	Value Drivers	Risk Drivers
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.	• Effective training programmes based on user feedback • Relevant training programmes • Enhanced quality of training programmes • Training content appropriately designed and structured to help users retain and reuse knowledge • Effective tracking/monitoring of costs (financial, material, etc.) and value added	• Inappropriate and ineffective training programmes selected • Outdated training material used • Decreasing quality of end-user training programmes • Training content design and structure failing to assist knowledge retention and reuse • Training cost outweighing its benefit and value-add

Test the Control Design

- Review the evaluation forms to verify that they effectively measure the quality and relevance of the contents and the level of the expectations met.
- Determine if feedback is summarised into a format useful for defining the future training curriculum.
- Obtain a list of follow-up actions and obtain evidence that they have been acted upon.
- Ensure that the target audience was reached.

Take the following steps to test the outcome of the control objectives:
- Review management communications to personnel encouraging additional education and self-study programmes.
- Obtain and review expense reimbursement requests for training.
- Obtain a list of vendor-provided training materials (e.g., manuals, CDs, training packets, syllabi).
- Obtain and review the inventory of educational books in the IT library.
- Speak with individual staff members to determine whether they have set a training plan that is aligned with their department's or the organisation's requirements.
- Inspect incident management records to identify trends in system support and usage that may indicate skill gaps.
- Enquire of management as to which specific competencies are required to support the environment, and ascertain whether there is a plan to build and maintain those skills for the organisation or to acquire those skills through third-party arrangements.
- Inspect a sample of individual performance plans to determine if technology training needs were incorporated.
- Enquire of management regarding results of performance evaluations and any potential skill gaps identified.
- Inspect problem management records to identify trends in system support and usage that may indicate skill gaps.
- Walk though the process for defining effective training programmes to determine if:
  - All relevant needs, including timing, are considered
  - Training sessions effectively meet training needs identified
  - Information on delivery mechanisms is up to date
  - Recent evaluations of trainers and programmes are reviewed
- Inspect the record of attendance and completion of training and education programmes for accuracy.
- Inspect the participant and trainer feedback from a sample of completed training sessions.
- Interview users to evaluate their understanding of the training sessions and then review the tests to verify that they effectively measure the quality and relevance of the contents of the sessions and the level of the expectations met.
- Enquire whether and confirm that stakeholders were interviewed and provided feedback on education and training.
- Enquire of management regarding results of performance evaluations and any potential skill gaps identified in areas where training has been delivered.
- Enquire of management and users whether user effectiveness and knowledge improved after the training was delivered.
- Determine whether indicators such as reduced number of service desk calls and productivity of users are assessed to indicate whether training had the intended impact.
- Inspect course evaluations to determine the degree of trainee satisfaction with the training delivered. Specifically consider the satisfaction with the instructors, course content and course location.

Take the following steps to document the impact of the control weaknesses:
- Obtain personnel files/résumés to analyse whether skills are appropriate for the job/position.
- Obtain personnel files/résumés to analyse skills against deployed systems.
- Enquire of management and review reports (e.g., listings of month-end and year-end accounting and reporting corrections) to determine whether corrections of information processed are required. Analyse to determine whether the incorrect information was caused by inadequate knowledge of users.
- Determine aggregate costs associated with downtime in areas where training or skills are undefined, and compare them to service costs for other areas or against peer groups.
- Inspect incident management records to identify trends in system support and usage that may indicate skill gaps.
- Enquire of management regarding results of performance evaluations and any potential skill gaps identified, such as in areas where training has been delivered.
- Assess benchmark indicators such as reduced number of service desk calls and productivity of users to indicate whether training had the intended impact.

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 Objective	Value Drivers	Risk Drivers
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.	• Increased customer satisfaction • Defined and measurable service desk performance • Incidents reported, followed up and solved in a timely manner	• Increased downtime • Decreased customer satisfaction • Users unaware of the follow-up procedures on reported incidents • Recurring problems not addressed

Test the Control Design

- Enquire whether and confirm that an IT service desk exists.
- Enquire whether and confirm that analysis has been performed to determine the service desk model, staffing, tools and integration with other processes.
- Confirm that the hours of operation and expected response time to a call meet business requirements.
- Enquire whether and confirm that instructions exist for the handling of a query that cannot be immediately resolved by service desk staff. Queries should have priority levels that determine the desired resolution time and escalation procedures.
- Ask relevant personnel about whether tools for the service desk are implemented in accordance with service definitions and SLA requirements.
- Enquire about the existence of standards of service and communication of the standards with customers.

DS8 Manage Service Desk and Incidents (cont.)

Control Objective	Value Drivers	Risk Drivers
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.	• Efficient solving of incidents in a timely manner • Added value for end users • Accountability for incident solving	• Not all incidents tracked • Prioritisation of incidents failing to reflect business needs • Incidents not solved in a timely manner

Test the Control Design

- Confirm that processes and tools are in place to register customer queries, status and actions toward resolution.
- Assess how completely and accurately this repository is maintained.
- Confirm that the process includes workflow for the handling and escalation of customer queries.
- Review a sample of open and closed customer queries to check compliance with the process and service commitments.

Control Objective	Value Drivers	Risk Drivers
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.	• Increased customer satisfaction • Consistent process for problem solving • Accountability for resolved incident • Clear track on incident resolution progress	• Inefficient use of resources • Unavailability of service desk resources • Inability to follow up incident resolution

Test the Control Design

- Enquire whether and confirm that the service desk maintains ownership of customer-related requests and incidents.
- Verify that the end-to-end life cycle of requests/incidents is monitored and escalated appropriately by the service desk.
- Confirm with members of management that significant incidents are reported to them.
- Review procedures for reporting significant incidents to management.
- Confirm the existence of a process to ensure that the incident records are updated to show the date and time of and the assignment of IT personnel to each query.
- Enquire whether and confirm that there is a process in place to ensure that IT staff members are involved in dealing with queries and incidents and that the incident request records are updated throughout the life cycle.

DS8 Manage Service Desk and Incidents (cont.)

Control Objective	Value Drivers	Risk Drivers
DS8.4 Incident Closure Establish procedures for the monitoring of timely 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.	• Increased customer satisfaction • Consistent and systematic incident resolution process • Prevention of problem recurrence	• Incorrect information gathering • Common incidents not solved properly • Incidents not resolved on a timely basis

Test the Control Design

- Enquire whether and confirm that a process is in place to manage the resolution of each incident.
- Enquire whether and confirm that all resolved incidents are described in detail, including a detailed log of all steps to resolve the incidents.
- Inspect a sample of incidents and verify that the status of managing the life cycle of the incident, including resolution and closure, is reported.

Control Objective	Value Drivers	Risk Drivers
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.	• Decreased service downtime • Increased customer satisfaction • Confidence in the offered services • Help desk performance measured and optimised	• Service desk activity failing to support business activities • Customers not satisfied by the offered services • Incidents not solved in a timely manner • Increasing customer downtime

Test the Control Design

- Enquire whether and confirm that a process is in place to identify, further investigate and report on all queries where the agreed-upon time frames for resolution have been exceeded.
- Enquire whether and confirm that trend analysis is being performed on all queries to identify repeating incidents and patterns, in support of problem identification.
- Verify if problem management is regularly provided with incident and trend analysis data.
- Enquire whether and confirm that the analysis is performed on the feedback received from customers to evaluate the levels of satisfaction with the service provided by the service desk.
- Confirm the existence of customer feedback analysis reports, and verify whether corrective actions have been taken to improve service.
- Confirm that service desk performance is compared to industry standards.
- Verify whether benchmark analysis is used for continuous improvement.

Take the following steps to test the outcome of the control objectives:
- Confirm how customers and users are advised of the service desk standards, and inspect the existence of these methods (postings at the service desk or online, etc.).
- Confirm the existence of user feedback logs.
- Enquire about the effectiveness of the system in terms of monitoring and improving customer satisfaction rates.
- Enquire about the existence of service desk performance reports.
- Inspect a sample of entries in the call log that were not immediately resolved, and determine whether the proper escalation procedures were followed.
- Inspect whether reported metrics address the relevant service desk goals. Enquire as to who uses the reports and for what purpose.
- Monitor several service desk calls to confirm whether existing procedures are being followed. Trace observed calls to the service incident tracking system.
- Enquire whether and confirm that incidents are properly prioritised according to policy.
- Review a sample of incident tickets to verify adherence to policy.
- Select a sample query and verify that incident records are updated to show the date and time of and the assignment of IT personnel to each query.
- Inspect samples of documentation of trouble incidents, and confirm that such incidents conform to priority levels set by policy.
- Enquire whether and confirm that users are informed on the progress of incident resolution.
- Enquire whether and confirm that all request and incident records are monitored through their life cycle and reviewed on a regular basis to guarantee a timely resolution of customer queries.
- Enquire whether and confirm that requests and incidents are closed only after confirmation of the requester.
- Inspect a sample of incidents and verify that there has been a manual or automated follow-up of the resolution.
- Confirm through inspection that incidents are reviewed for update in the knowledge base, including workarounds, known errors and the root cause for similar incidents arising in the future. Physically inspect the knowledge base, and inspect a sample of entries to ensure that the workaround is included, as well as the root cause, if known.
- Inspect a sample of incident records, and verify if they were monitored and fulfiled according to SLAs.
- Select a sample of records and confirm with the requester that they were consulted for closure.
- Identify whether appropriate definitions exist for incident classification (e.g., by impact and urgency).
- Identify whether procedures for functional and hierarchical escalation are defined.
- Enquire whether and confirm that incident management is clearly linked with continuity/contingency plans.

Take the following steps to document the impact of the control weaknesses:
- Observe several service desk calls to confirm undocumented procedures. Undocumented escalation procedures should assign trouble tickets that the service desk cannot resolve to the appropriate IT staff members.
- Verify that all critical service calls are prioritised by the service desk manager or a senior staff member.
- Observe operations of the IT support team, and record undocumented procedures to log and prioritise incidents.

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 Objective	Value Drivers	Risk Drivers
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.	• Hardware and software planned effectively to maintain business services • The configuration deployed consistently across the enterprise • Planning enhanced so that changes are in accordance with the overall architecture • Cost savings through supplier consolidation • Fast incident resolution	• Failure of changes to comply with the overall technology architecture • Assets not protected properly • Unauthorised changes to hardware and software not discovered, which could result in security breaches • Documented information failing to reflect the current architecture • Inability to fall back

Test the Control Design

- Enquire whether and confirm that senior management sets scope and measures for configuration management functions, and assesses performance.
- Enquire whether and confirm that a tool is in place to enable the effective logging of configuration management information in a repository.
- Determine that access to the tool is restricted to appropriate personnel.
- Review a sample of configuration items to ensure that a unique identifier is assigned.
- Enquire whether and confirm that configuration baselines for components are defined and documented.
- Review that baselines enable identification of system configuration at discrete points in time.
- Enquire whether and confirm that there is a documented process to revert to the baseline configuration.
- Test a sample of systems and applications by verifying that they can be reverted to baseline configurations.
- Enquire whether and confirm that mechanisms exist to monitor changes against the defined repository and baseline.
- Verify that management is receiving regular reports and that these reports result in continuous improvement plans.

DS9 Manage the Configuration (cont.)

Control Objective	Value Drivers	Risk Drivers
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.	• Effective change and incident management • Compliance with accounting requirements	• Failure to identify business-critical components • Uncontrolled change management, causing business disruptions • Inability to assess the impact of a change because of inaccurate information • Inability to accurately account for assets

Test the Control Design

- Enquire whether and confirm that a policy is in place to ensure that all configuration items and their attributes are identified and maintained.
- Enquire whether and confirm that there is a policy for physical asset tagging.
- Verify that assets are physically tagged according to policy.
- Enquire whether and confirm that a role-based access policy exists.
- Verify that authorised and appropriate personnel have designated access to the configuration repository as per the policy.
- Enquire whether and confirm that a policy is in place to ensure that change and problem management procedures are integrated with the maintenance of the configuration repository.
- Enquire whether and confirm that a process is in place to record new, modified and deleted configuration items, and identify and maintain the relationships amongst configuration items in the configuration repository.
- Inspect relevant documentation, timely execution and data integrity of the process.
- Enquire whether and confirm that a process is in place to ensure that analysis is done to identify critical configuration items.
- Verify that this process supports change management and analysis of future processing demands and technology acquisitions.
- Enquire whether and confirm that procurement procedures provide for the recording of new assets within the configuration management tool.
- Validate that the confirmation management data match the procurement records.

DS9 Manage the Configuration (cont.)

Control Objective	Value Drivers	Risk Drivers
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.	• Identification of deviations from the baseline • Enhanced identification and solving of problems • Identification of unauthorised software	• Failure to identify business-critical components • Uncontrolled change management, causing business disruptions • Misused assets • Increased costs for problem solving

Test the Control Design

- Enquire whether and confirm that a process is in place to regularly ensure the integrity of all configuration data.
- Review reports that compare recorded data against the physical environment.
- Verify that deviations are reported and corrected.
- Verify that hardware and software reconciliation is periodically performed against the configuration database.
- If automated tools are being used, perform a manual reconciliation against the automated record.
- Verify that periodic reviews are performed against the policy for software usage to detect personal, unlicensed software or any software instances in excess of current license agreements.

Take the following steps to test the outcome of the control objectives:
- Enquire of management whether any failed configuration changes or security breaches have occurred, and ascertain whether those issues resulted in a loss of corporate assets, disclosure information or downtime. Determine that access to the logging tool is restricted to appropriate personnel.
- Review a sample of configuration items to ensure that a unique identifier is assigned.
- Verify that baselines enable identification of system configuration at discrete points in time.
- Enquire whether and confirm that there is a documented process to revert to the baseline configuration.
- Inspect the outputs of tools designed to detect changes to the configuration, and assess whether those changes are in alignment with the organisation's design specifications and security strategy.
- Inspect the tools used for the configuration management database (CMDB), and verify that the quantity and quality of information provided by the CMDB are appropriate for all IT processes.
- Determine whether configuration information is held in redundant information systems.
- Select a sample of desktops and examine the configuration and software deployed against baseline standards to ensure that no unauthorised changes have been made.
- Identify whether the use of unlicensed software is prevented and procedures exist to detect unauthorised software.
- Verify that management is receiving regular reports and that these reports result in continuous improvement plans.
- Test a sample of systems and applications by verifying that they can be reverted to baseline configurations.
- Obtain vulnerability assessment tools for deployed technologies, and run them to determine whether known vulnerabilities have been corrected.
- Determine what should be documented (e.g., configuration items, incident records, change records, change schedules, availability information, service levels) for the review of configuration information and to document the relationship amongst configuration items.

Take the following steps to document the impact of the control weaknesses:
- Enquire of management if any failed configuration changes or security breaches have occurred, and ascertain whether those issues have resulted in a loss of corporate assets, disclosure information or downtime.
- Inspect copies of internal or external reports on configuration assessments, and determine whether configuration weaknesses have been identified.
- Use vulnerability assessment tools for deployed technologies to determine whether known vulnerabilities have been corrected.

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.

Control Objective	Value Drivers	Risk Drivers
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.	• Support tools for service desk performance • Proactive problem management • Enhanced end-user training • Efficient and effective problem and incident handling • Problems and incidents solved in a timely manner • Improved quality of IT services	• Disruption of IT services • Increased likelihood of problem recurrence • Problems and incidents not solved in a timely manner • Lack of audit trails of problems, incidents and their solutions for proactive problem and incident management • Recurrence of incidents

Test the Control Design

- Enquire whether and confirm that adequate processes supported by appropriate tools are in place to identify and classify problems.
- Review established criteria to classify and prioritise problems, ensuring that they result in classifications in line with service commitments and organisational units responsible for resolving or containing the problem.
- Confirm that a process is in place for the accuracy of classification, and identify reasons for misclassification so they can be addressed.
- Take a representative sample from the problem database to ensure that the problems are appropriately classified and categorised.

DS10 Manage Problems (cont.)

Control Objective	Value Drivers	Risk Drivers
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 request for change (RFC) or to implement an urgent change as appropriate. Monitor the progress of problem resolution against SLAs.	• Limited disruption to or reduction of IT service quality • Efficient and effective handling of problems and incidents • Minimised elapsed time for problem detection to resolution • Appropriate problem solving with respect to the agreed-upon service levels • Improved quality of IT services	• Recurrence of problems and incidents • Loss of information • Critical incidents not solved properly • Business disruptions • Insufficient service quality

Test the Control Design

- Confirm that processes and tools are in place to register, classify, prioritise and track problems to resolution.
- Confirm that tools include reporting facilities that are used to produce management reports on problems.
- Select a sample of problem reports and verify the adequacy of:
  - Problem documentation for analysis of root causes
  - Identification of problem ownership and resolution responsibility
  - Problem status information

DS10 Manage Problems (cont.)

Control Objective	Value Drivers	Risk Drivers
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.	• Queries resolved within the agreed-upon time frames • Improved customer and user satisfaction • Efficient and effective problem and incident handling • Ability to apply lessons learned when addressing future problems similar in nature	• Outstanding queries • Increased service disruption • Critical incidents not solved properly • Dissatisfaction with IT services

Test the Control Design

- Enquire whether and confirm that problems are closed only after confirmation of resolution by the stakeholders.
- Select a representative sample of problems and verify through interviews with stakeholders that the stakeholders were informed completely and in a timely manner of problem closures.

Control Objective	Value Drivers	Risk Drivers
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.	• Improved customer satisfaction • Efficient and effective problem and incident handling • Documented problem and incident reporting • Effective service management	• Loss of information • Critical incidents not solved properly • Business disruptions • Increasing number of problems • Decreased satisfaction with IT services

Test the Control Design

- Review the processes for configuration, incident and problem management, and confirm that they are appropriately integrated.
- Review records to confirm that the responsible managers of the different areas regularly meet and resolve common issues.

Take the following steps to test the outcome of the control objectives:
- Compare the incident list to incident reports and error logs to ensure that the incident process is working correctly.
- Verify the existence of problem identification and handling documentation.
- Inspect a sample of reports to ensure that they are being used when appropriate and that they contain the necessary information.
- Verify that known errors, incident analysis tools and root causes are communicated to the incident management processes.
- Verify that the status of the problem handling process is monitored throughout its life cycle, including input from change and configuration management.
- Review schedules and minutes of meetings amongst process owners for configuration, incident and problem management.
- Inspect and review records and reports regarding the total costs of problems.

Take the following step to document the impact of the control weaknesses:
- Enquire whether and confirm that changes resulting from the problem management process are monitored to determine the overall improvement of IT services.

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.

Control Objective	Value Drivers	Risk Drivers
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 data processing restart and reprocessing needs.	• Data management in support of business requirements • Guidance for data handling • Data transactions authorised • Safeguarded storage of sources	• Data management failing to support business requirements • Security breaches • Business, legal and regulatory requirements not met

Test the Control Design

- Obtain the inventory of data elements.
- For each data element, confirm that requirements for confidentiality, integrity and availability have been defined and that these requirements have been validated with the data owners.
- Ensure that controls commensurate with requirements have been defined and implemented.

Control Objective	Value Drivers	Risk Drivers
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.	• Data management in support of business requirements • Guidance for data handling • Safeguarded storage of sources • Data retrieved in an efficient manner	• Data not protected from unauthorised viewing or altering • Documents not retrieved when needed • Non-compliance with regulatory and legal obligations • Unauthorised data access

Test the Control Design

- Review the data model, and ensure that storage techniques satisfy business requirements.
- Review retention periods for data, and ensure that they are in line with contractual, legal and regulatory requirements.

DS11 Manage Data (cont.)

Control Objective	Value Drivers	Risk Drivers
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.	• Accounting of all media • Improved backup management • Safeguarding of data availability • Reduced time for data restoration	• Media integrity compromised • Backup media unavailable when needed • Unauthorised access to data tapes • Destruction of backups • Inability to determine location of backup media

Test the Control Design

- Obtain the media inventory and, on a sample basis, ensure that media on the inventory list can be identified and items in storage can be traced back to the inventory.
- On a sample basis, confirm that external labels correspond with internal labels, or otherwise validate that external labels are affixed to the correct media.

Control Objective	Value Drivers	Risk Drivers
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.	• Proper protection of corporate information • Enhanced backup management • Safeguarding of data availability	• Disclosure of corporate information • Compromised integrity of sensitive data • Unauthorised access to data tapes

Test the Control Design

- Enquire whether and confirm that:
  - Responsibility for the development and communication of policies on disposal is clearly defined
  - Equipment and media containing sensitive information are sanitised prior to reuse or disposal in such a way that data marked as ‘deleted’ or ‘to be disposed’ cannot be retrieved (e.g., media containing highly sensitive data have been physically destroyed)
  - Disposed equipment and media containing sensitive information have been logged to maintain an audit trail
  - There is a procedure to remove active media from the media inventory list upon disposal. Check that the current inventory has been updated to reflect recent disposals in the log.
  - Unsanitised equipment and media are transported in a secure way throughout the disposal process
  - Disposal contractors have the necessary physical security and procedures to store and handle the equipment and media before and during disposal

DS11 Manage Data (cont.)

Control Objective	Value Drivers	Risk Drivers
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.	• Corporate information properly restored • Enhanced backup management aligned with the business requirements and the backup plan • Safeguarding of data availability and integrity	• Disclosure of corporate information • Inability to recover backup data when needed • Recovery procedures failing to meet business requirements • Inability to restore data in the event of a disaster • Inappropriate time requirement for performing backups

Test the Control Design

- Enquire whether and confirm that:
  - Critical data that affect business operations are periodically identified in alignment with the risk management model and IT service continuity plan
  - Adequate policies and procedures for the backup of systems, applications, data and documentation exist and consider factors including:
    - Frequency of backup (e.g., disk mirroring for real-time backups vs. DVD-ROM for long-term retention)
    - Type of backup (e.g., full vs. incremental)
    - Type of media
    - Automated online backups
    - Data types (e.g., voice, optical)
    - Creation of logs
    - Critical end-user computing data (e.g., spreadsheets)
    - Physical and logical location of data sources
    - Security and access rights
    - Encryption
  - Responsibilities have been assigned for taking and monitoring backups
  - A schedule exists for taking and logging backups in accordance with established policies and procedures
  - System, application, data and documentation maintained or processed by third parties are adequately backed up or otherwise secured. The return of backups from third parties should be required and escrow or deposit arrangements considered.
  - Requirements for onsite and offsite storage of backup data have been defined that meet the business requirements, including the access required to backup data
  - Sufficient restoration tests have been performed periodically to ensure that all components of backups can be effectively restored
  - The time frame required for restoration has been agreed upon and communicated with the business or IT process owner. The priority for data recovery has been based on business requirements and IT service continuity procedures.

DS11 Manage Data (cont.)

Control Objective	Value Drivers	Risk Drivers
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.	• Sensitive information properly secured and protected • Ability to view or alter information available to authorised users • Completeness and accuracy of transmitted data	• Sensitive data misused or destroyed • Unauthorised data access • Incompleteness and inaccuracy of transmitted data • Data altered by unauthorised users

Test the Control Design

- Enquire whether and confirm that:
  - A process is in place that identifies sensitive data and addresses the business need for confidentiality of the data, compliance with applicable laws and regulations has been addressed, and the classification of data has been agreed upon with the business process owners
  - A policy has been defined and implemented to protect sensitive data and messages from unauthorised access and incorrect transmission and transport, including, but not limited to, encryption, message authentication codes, hash totals, bonded couriers and tamper-resistant packaging for physical transport
  - Requirements have been established for physical and logical access to data output, and confidentiality of output is clearly defined and taken into consideration
  - Rules and procedures have been established for end-user access to data and management and backup of sensitive data
  - Rules and procedures have been established for end-user applications that may adversely impact data stored on end-user computers or networked applications or data (e.g., consider policies on user rights on networked personal computers)
  - Awareness programmes have been instituted to create and maintain awareness of security in the handling and processing of sensitive data
  - Sensitive information processing facilities are within secure physical locations protected by defined security perimeters coupled with appropriate surveillance, security barriers and entry controls
  - The design of the physical infrastructure prevents losses from fire, interference, external attack or unauthorised access. There are secure output dropoff points for sensitive outputs or transfer of data to third parties.

Take the following steps to test the outcome of the control objectives:
- Review business requirements documentation to ensure that the documentation mechanism is being used as designed.
- Inspect the data management tools to make sure that they are being used as described.
- Verify that access to media and systems is restricted to authorised personnel.
- Verify if media that are susceptible to degradation, such as tape, are routinely replaced.
- Select a sample of the media disposal list and verify that the disposed media are not on the media inventory list.
- Inspect on- and offsite storage facilities and check for accessibility.
- Review a sample of test results to ensure that restorations are successful and the time required for restoration is reconciled with SLAs and continuity requirements.
- Verify that backup information is stored offsite, as required by continuity processes.
- Verify that procedures to ensure integrity of archived information are in place and followed.

Take the following steps to document the impact of the control weaknesses:
- Enquire whether and confirm that a policy is in place that meets business requirements for disposal or reuse of equipment and media to minimise the risk of exposure of sensitive data to unauthorised persons.
- Enquire whether and confirm that critical data that affect business operations are periodically identified, in alignment with the risk management model and IT service continuity plan.
- Verify that consideration is given to the confidentiality, integrity and availability of the data as well as applicable laws and regulations.

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.

Control Objective	Value Drivers	Risk Drivers
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.	• Minimised threats to physical security • Decreased risk of a physical attack on the IT site via reduction of the possibility of the site being identified by unauthorised persons who may initiate such an attack • Reduction in insurance costs as a result of demonstrating optimal physical security management	• Threats to physical security not identified • Increased vulnerability to security risks, resulting from site location and/or layout

Test the Control Design

- Enquire whether and confirm that:
  - Physical sites for IT equipment have been selected according to a technology strategy that meets business requirements and a security policy, considering such issues as geographic position, neighbours, infrastructure and risks (e.g., theft, temperature, fire, smoke, water, vibration, terrorism, vandalism, chemicals, explosives)
  - A process is defined and implemented that identifies the potential risks and threats to the organisation's IT sites and assesses the business impact on an ongoing basis, taking into account the risk associated with natural and man-made disasters
  - The selection and design of the site take into account relevant laws and regulations, such as building codes; environmental, fire, electrical engineering; and occupational health and safety regulations

DS12 Manage the Physical Environment (cont.)

Control Objective	Value Drivers	Risk Drivers
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.	• Protection of critical IT systems from physical threats • Effective deployment of physical security measures • Promotion of awareness amongst staff and management of the organisation's requirements for physical security	• Threats to physical security not identified • Hardware stolen by unauthorised people • Physical attack on the IT site • Devices reconfigured without authorisation • Confidential information being accessed by devices configured to read the radiation emitted by the computers

Test the Control Design

- Enquire whether and confirm that:
  - A policy is defined and implemented for the physical security and access control measures to be followed for IT sites. The policy is regularly reviewed to ensure that it remains relevant and up to date.
  - Access to information about sensitive IT sites and their design plans is limited
  - External signs and other identification of sensitive IT sites are discreet and do not obviously identify the site from outside
  - Organisational directories/site maps do not identify the location of the IT site
  - The design of physical security measures takes into account the risks associated with the business and operation. Where appropriate, physical security measures include alarm systems, building hardening, armoured cabling protection, secure partitioning, etc.
  - Tests of the preventive, detective and corrective physical security measures are performed periodically to verify design, implementation and effectiveness
  - The site design takes into account the physical cabling of telecommunication and piping of water, power and sewer
  - A process supported by the appropriate authorisation is defined and implemented for the secure removal of IT equipment
  - Receiving and shipping areas of IT equipment are safeguarded in the same manner and scope as normal IT sites and operations
  - A policy and process are defined to transport and store equipment securely
  - A process exists to ensure that storage devices containing sensitive information are physically destroyed or sanitised
  - A process exists for recording, monitoring, managing, reporting and resolving physical security incidents, in line with the overall IT incident management process
  - Particularly sensitive sites are checked frequently (including weekends and holidays) by security personnel

DS12 Manage the Physical Environment (cont.)

Control Objective	Value Drivers	Risk Drivers
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.	• Appropriate access to ensure timely resolution of a critical incident • All visitors identifiable and traceable • Staff aware of responsibilities in respect to visitors	• Visitors gaining unauthorised access to IT equipment or information • Unauthorised entry to secure areas

Test the Control Design

- Enquire whether and confirm that:
  - A process is in place that governs the requesting and granting of access to the computing facilities
  - Formal access requests are completed and authorised by management of the IT site, the records are retained, and the forms specifically identify the areas to which the individual is granted access. This is verified by observation or review of approvals.
  - Procedures are in place to ensure that access profiles remain current. Verify that access to IT sites (server rooms, buildings, areas or zones) is based on job function and responsibilities.
  - There is a process to log and monitor all entry points to IT sites, registering all visitors, including contractors and vendors, to the site
  - A policy exists instructing all personnel to display visible identification at all times and prevents the issuance of identity cards or badges without proper authorisation. Observe whether badges are being worn in practice.
  - A policy exists requiring visitors to be escorted at all times by a member of the IT operations group whilst onsite, and individuals who are not wearing appropriate identification are pointed out to security personnel
  - Access to sensitive IT sites is restricted through perimeter restrictions, such as fences/walls and security devices on interior and exterior doors. Verify that the devices record entry and sound an alarm in the event of unauthorised access. Examples of such devices include badges or key cards, key pads, closed-circuit television and biometric scanners.
  - Regular physical security awareness training is conducted. Verify by reviewing training logs.

DS12 Manage the Physical Environment (cont.)

Control Objective	Value Drivers	Risk Drivers
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.	• Identification of all potential environmental threats to the IT facilities • Prevention or timely detection of environmental threats • Reduced risk of claims against insurance companies being rejected for non-compliance with the requirements of insurance policies, and minimised insurance premiums • Appropriate protection against environmental factors	• Facilities exposed to environmental impacts • Inadequate environmental threat detection • Inadequate measures for environmental threat protection

Test the Control Design

- Enquire whether and confirm that:
  - A process is in place to identify natural and man-made disasters that might occur in the area within which the sensitive IT facilities are located. Review reports to verify that the potential impact is assessed according to business continuity planning procedures.
  - A policy is in place that outlines how IT equipment, including mobile and offsite equipment, is protected against theft and environmental threats. Review documentation to ensure that the policy, for example, bars eating, drinking and smoking in sensitive areas, and prohibits storage of stationery and other supplies posing a fire hazard within computer rooms.
  - IT facilities are situated and constructed in a way to minimise and mitigate susceptibility to environmental threats
  - Suitable devices are in place that will detect environmental threats. Inspect continuous monitoring done at these devices.
  - Alarms or other notifications are raised in case of an environmental exposure, procedures in response to such occurrences are documented and tested, and personnel are given suitable training
  - A process is in place to compare measures and contingency plans against insurance policy requirements. Review the reports and the insurance policy to verify compliance.
  - Management takes action to ensure that any points of non-compliance are addressed in a timely manner
  - IT sites are built in locations that minimise the impact of environmental risk, such as theft, air, fire, smoke, water, vibration, terrorism and vandalism. Physically inspect the locations of the IT sites to ensure that the design is properly implemented. Review the risk assessment report made prior to the design and construction of the site.
  - A policy is in place to ensure ongoing cleaning and clean-up in proximity of IT operations. Check the IT sites and server rooms to make sure that they are kept in a clean, tidy and safe condition at all times (e.g., no mess/litter, paper or cardboard boxes, filled dustbins, flammable chemicals or materials). Enquire whether the sites are always kept clean.

DS12 Manage the Physical Environment (cont.)

Control Objective	Value Drivers	Risk Drivers
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.	• Protection of critical IT systems from the effects of power outages and other facility-related risks • Effective and efficient use of facility resources	• Non-compliance with health and safety regulations • IT systems failure due to improper protection from power outages and other facility-related risks • Accidents to staff members

Test the Control Design

- Enquire whether and confirm that:
  - A process exists that examines the IT facilities' need for protection against environmental conditions and power fluctuations and outages, in conjunction with other business continuity planning procedures
  - Uninterruptible power supplies (UPSs) are acquired and meet availability and business continuity requirements
  - A process is in place to regularly test the UPS's operation and to ensure that power can be switched to the supply without any significant effect on business operations
  - The tests have been performed and corrective action is taken where needed
  - In facilities housing sensitive IT systems, more than one power supply entry is available
  - The physical entrance of power is separated
  - Cabling external to the IT site is located underground or has suitable alternative protection
  - Blueprints and plans exist
  - Cabling within the IT site is contained within secured conduits
  - Cabling is protected and hardened against environmental risk
  - Wiring cabinets are locked with restricted access
  - Cabling and physical patching (data and phone) are well structured and organised
  - Documentation for cabling and conduits is available for reference
  - For facilities housing high-availability systems, analysis is done for redundancy and fail-over cabling requirements (external and internal)
  - A process is in place to ensure that IT sites and facilities are in ongoing compliance with relevant health and safety laws, regulations, guidelines, or vendor specifications
  - A process is in place to educate personnel on health and safety laws, regulations or guidelines. This also includes education of personnel on fire and rescue drills to ensure knowledge and actions made in case of fire or similar incidents.
  - The training programme assesses knowledge of the guidelines and the training programme is documented
  - A process is in place to record, monitor, manage and resolve facilities incidents in line with the IT incident management process
  - Reports on incidents are made available where disclosure is required in terms of laws and regulations
  - A process is in place to ensure that IT sites and equipment are maintained per the supplier's recommended service intervals and specifications
  - Maintenance is carried out only by authorised personnel. Review documentation and enquire of personnel to confirm.
  - Physical alterations to IT sites or premises are analysed to reassess the environmental risk (e.g., fire, water damage)
  - Results of this analysis are reported to business continuity and facilities management
- Walk through the facilities and compare findings with the health and safety guidelines.
- Enquire of personnel about possible breaches of the standards.
- Walk through recently changed sites to ensure that they still meet standards for risks.

Take the following steps to test the outcome of the control objectives:
- Review the risk analysis report to verify that the report has been updated within the last year.
- Review policies to verify that new/updated regulations and laws are reflected in the policies.
- Walk through the areas to ensure that they are secure according to procedures.
- Review the security logs for confirmation of minimum security checks.
- Inspect the logs to verify that they include, at minimum, the visitor's name, the visitor's company, the purpose of the visit, the name of the member of the IT operations group authorising the visit, the date of visit, and the times of entry and exit.
- Select a sample of personnel with badges and verify authorisiation.
- Verify whether wiring cabinets are locked and have restricted access.
- Verify that documentation for cabling and conduits is available for reference.
- Walk through the facilities and compare findings with the health and safety guidelines.
- Interview personnel to assess their knowledge of the guidelines.

Take the following steps to document the impact of the control weaknesses:
- Verify that special considerations are taken into account (e.g., geographic position, neighbours, infrastructure). Other risks that need consideration are theft, temperature, fire, smoke, water, vibration, terrorism, vandalism, chemicals and explosives.
- Enquire whether and confirm that a process exists that examines the IT facilities' need for protection against environmental conditions and power fluctuations and outages, in conjunction with other business continuity planning procedures.

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.

Control Objective	Value Drivers	Risk Drivers
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.	• Demonstration that IT operations are meeting SLAs • Promotion of continuity of operational support by documenting staff experience and retaining it in a knowledge base • Structured, standardised and clearly documented IT operations procedures and support staff instructions • Reduced time to transfer knowledge between skilled operation support staff and new recruits	• Errors and rework due to misunderstanding of procedures • Inefficiencies due to unclear and/or non-standard procedures • Inability to deal quickly with operational problems, new staff and operational changes

Test the Control Design

- Inspect a copy of the standard IT operational procedures.
- Review operational procedures for completeness. Content may include roles and responsibilities of IT staff members, organisation charts, direct supervisor roles and reports, procedures for abnormal operating system termination, a callout list in the case of emergency, etc.
- Inspect the organisation chart and review job roles.

Control Objective	Value Drivers	Risk Drivers
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.	• Optimised use of system resources by equalising loads and minimising the impact to online users • Minimised effect of changes to job schedules to avoid production disruptions	• Resource utilisation peaks • Problems with scheduling of *ad hoc* jobs • Reruns or restarts of jobs

Test the Control Design

- Enquire whether and confirm that:
  - Batch job execution procedures are complete
  - Procedures include an expected daily job schedule, point of contacts in the case of job failures and a running list of job failure codes
  - Batch job duties and responsibilities for each computer operator exist
  - Computer operator shift schedules exist
  - Schedules include start and end shifts and names of the operators
  - At least one operator is present during the execution of batch jobs

DS13 Manage Operations (cont.)

Control Objective	Value Drivers	Risk Drivers
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.	• Proactive detection of infrastructure problems likely to result in an incident • Ability to monitor trends and deal with potential infrastructure problems before they occur • Ability to optimise the deployment and use of resources	• Infrastructure problems undetected and occurrence of incidents • Infrastructure problems causing greater operational and business impact than if they had been prevented or detected earlier • Poorly utilised and deployed infrastructure resources

Test the Control Design

- Enquire whether and confirm that:
  - A planned process for event logging identifies the level of information to be recorded based on a consideration of risk and performance
  - Infrastructure assets that need to be monitored are identified based on service criticality and the relationship between configuration items and services that depend on them
  - Documentation of the process plan for logging exists. Physically inspect the documents.
  - The list of assets properly identifies the assets. Enquire of personnel as to what assets are most important, and trace those assets to the list.

Control Objective	Value Drivers	Risk Drivers
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.	• Additional protection for special forms and commercially sensitive output data through inventory management • Prevention of theft, fraud, tampering, destruction or other abuses of sensitive IT assets • Verification of access authorisations before granting physical access to special forms and output devices, and retention of evidence regarding the integrity of special output devices	• Misuse of sensitive IT assets, leading to financial losses and other business impacts • Inability to account for all sensitive IT assets

Test the Control Design

- Enquire whether and confirm that:
  - Procedures exist to govern the receipt, removal and disposal of special forms and output devices into, within and out of the organisation
  - At least a semi-annual review exists of access to sensitive assets
  - A procedure exists to gain, change and remove access to sensitive assets
  - Removal and disposal procedures documentation exists

DS13 Manage Operations (cont.)

Control Objective	Value Drivers	Risk Drivers
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.	• Optimised system performance and availability • Preventive incident and problem management • Protection of warranties	• Infrastructure problems that could have been avoided or prevented • Warranties violated due to non-compliance with maintenance requirements

Test the Control Design

- Enquire whether and confirm that:
  - A preventive maintenance plan for all critical hardware is in place and that it is designed considering cost-benefit analysis, vendor recommendations, risk of outage, qualified personnel and other relevant factors
  - Activity logs are reviewed for identification of preventive maintenance needs, and the expected impact (e.g., performance restrictions, SLAs) of maintenance activities is communicated to affected customers and users

Take the following steps to test the outcome of the control objectives:

- Enquire whether and confirm that standard IT operational procedures that support agreed-upon service levels are in place. Procedures should include a trouble escalation system to track and monitor downtime.
- Enquire whether and confirm that roles and responsibilities, including those of external service providers, are defined. Review any relevant documentation for existence.
- Enquire whether and confirm that support staff members are aware of and understand the operations procedures and related tasks for which they are responsible. Walk through the support staff work area to confirm that the operations processes are being implemented correctly.
- Enquire whether and confirm that the procedures are consistently maintained and implemented properly by reviewing logs.
- Enquire whether and confirm that handover communications and related responsibilities are defined.
- Enquire whether and confirm that procedures for exception handling exist and are integrated with incident management.
- Confirm job and role descriptions for segregation of duties. For example, computer operators should not have access to the programs, and computer programmers should not have access to production data or write directly to the media (BLP, bypass label processing).
- Verify the existence of documentation of the procedures. Observe and interview staff members to verify adherence to the procedures.
- Inspect access privileges to verify that segregation of duties is appropriate.
- Inspect documentation and interview operational staff members to verify that procedures are followed.
- Observe operational staff members to confirm use of procedures and document performance.
- Enquire whether and confirm that scheduling of batch jobs is controlled by the use of job scheduling software. Ensure that proper security controls are in place to prevent unauthorised jobs from running.
- Enquire whether and confirm that batch jobs are scheduled.
- Evaluate the scheduling process to ensure that the scheduling of batch jobs takes into consideration:
  - Business requirements
  - Priority of job
  - Conflicts between jobs
  - Workload balancing (performance and capacity management)
- Enquire whether and confirm that the outcomes of batch jobs are monitored and verified.
- Enquire whether and confirm that automated processes are in place to immediately notify when batch jobs fail. Inspect hardware and software related to the automated processes to verify existence.
- Ensure that control of batch jobs is not limited to technical information (e.g., time required to complete the job) and that business process requirements for the data are controlled (e.g., completeness and correctness of data processed).
- Inspect relevant documentation for existence and to ensure that the formal procedures properly address the scheduling of batch jobs.
- Inspect change documentation to verify accuracy.
- Verify the existence of schedules.
- Inspect documentation and evidence that batch job incidents were raised and solved in a timely manner.
- Enquire whether and confirm that rules are defined covering thresholds and event conditions and are implemented within the system to ensure that real events are triggered when required.
- Enquire whether and confirm that event logs are produced and kept for an appropriate period to assist in future investigations and access control monitoring.
- Enquire whether and confirm that procedures for monitoring event logs are established, the results of the monitoring activities are reviewed regularly and, if appropriate, incidents are escalated to the service desk.
- Enquire whether and confirm that incidents are created for all deviations noted.
- Inspect event logs to ensure that they are not overloaded with minor events and that all major events are recorded.
- Inspect event logs to verify existence and appropriateness.
- Obtain a sample query of event log entries that may trigger a service desk ticket. Trace the event log entry to the service ticket logs.
- Enquire whether and confirm that access to sensitive documents and output devices is assigned appropriately.
- Enquire whether and confirm that a regular reconciliation of sensitive documents and devices is conducted. Perform a reconciliation of a sample of sensitive documents and devices, comparing actual to recorded amounts.
- Enquire whether and confirm that appropriate physical safeguards are established.
- Inspect and test the physical safeguards of sensitive assets.
- Inspect whether appropriate critical equipment is available.
- Enquire whether and confirm that all activity logs are reviewed on a regular basis, to identify critical hardware components that require preventive maintenance.
- Enquire whether and confirm that communication means are effective in informing users of the impact of outages immediately (e.g., e-mail, phone tree).
- Confirm with the business and IT that scheduling was performed in accordance to business requirements. Review the production schedule, and verify that all relevant equipment is considered and scheduling considers service requirements.

- Physically inspect the hardware to confirm that maintenance has been taking place. Inspect the plan to ensure that it is designed effectively considering cost-benefit analysis, vendor recommendations, risk of outage, qualified personnel and other relevant factors.
- Determine if appropriate action is taken in a timely manner for critical maintenance.

Take the following steps to document the impact of the control weaknesses:
- Enquire whether a lack of documented procedures impacts continuous operations, i.e., computer operators are able to conduct daily operations without an operations manual, and lines of communication are known.
- Enquire whether undocumented IT operations procedures reflect current operations. If not, it may hinder cross-training or training of new hires and lead to improper procedures being followed during a shift turnover.
- Enquire whether and confirm that all batch jobs are completed via reports or other means.
- Observe that computer operators are monitoring and completing batch jobs as scheduled.
- Enquire of IT staff members about the last service outage, and review the event log for existence. Confirm that proper documentation, including reason and resolution, is recorded.
- Inspect event logs for a week-long period to confirm existence and enquire of IT staff members of resolution of event log entries.
- Inspect access to sensitive assets, and confirm whether access to assets is appropriate by tracing access to organisation chart.
- Observe physical safeguards to assets, and determine whether such safeguards are appropriate.
- Physically inspect the hardware to confirm that maintenance has been taking place. Inspect the plan to ensure that it is designed effectively considering cost-benefit analysis, vendor recommendations, risk of outage, qualified personnel and other relevant factors.

Appendix V—
Monitor and Evaluate (ME)

ME1 Monitor and Evaluate IT Performance
ME2 Monitor and Evaluate Internal Control
ME3 Ensure Compliance With External Requirements
ME4 Provide IT Governance

APPENDIX V—MONITOR AND EVALUATE (ME)

PROCESS ASSURANCE STEPS

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 Objective	Value Drivers	Risk Drivers
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.	• A transparent view of IT's performance, based on reliable information • Opportunities for improvement identified • Facilitated achievement of business and governance requirements • Cost-efficient IT services • More informed IT investment decisions, improving value delivery • Consistent use and integrity of performance indicators	• Performance reports based on out-of-date, inaccurate or unreliable data • Performance metrics not aligned with business and governance requirements • Lack of timely identification of issues related to IT and business alignment • Customer expectations and business needs not adequately identified • Monitored data failing to support the analysis of the overall process performance

Test the Control Design

- Obtain and review management's definition of critical business processes, strategic initiatives and key IT processes to ensure that they support the corporate performance management system.
- Understand management's method of communicating its critical business processes, strategic initiatives and key IT processes.
- Confirm that there is a metrics-based monitoring approach for IT performance drivers (e.g., inspect corporate policies and other relevant documentation).
- Determine if the monitoring approach provides appropriate goal and performance indicators with efforts to instill ratios that bring important business issues to light.
- Identify whether appropriate systems are used to monitor IT performance.
- Interview members of management to identify their awareness of relationships and dependencies between IT processes when monitoring IT process activities (e.g., expectation gaps, undefined interfaces, 'things falling between the cracks', duplication of effort, inefficiencies).
- Understand management's approach regarding review over the relevance of interdependencies of key IT processes to align with business goals and objectives.

ME1 Monitor and Evaluate IT Performance (cont.)

Control Objective	Value Drivers	Risk Drivers
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.	• Identification and measurement of the most critical and meaningful metrics • Strong customer bias in the culture of the IT organisation for all IT processes • Improved customer satisfaction and focus • Ability of systems to efficiently provide the data required to monitor the processes • A history of organisational performance to monitor trends and changes in performance	• Metrics based on objectives that are not aligned with business objectives • Metrics based on incorrect or incomplete data • Ineffective reporting on organisationwide IT process performance indicators • Customer expectations and business needs not identified • Monitored data failing to support the analysis of the overall process performance

Test the Control Design

Enquire whether and confirm that:
- Targets have been defined for the IT metrics in line with the coverage and characteristics of the metrics defined in the monitoring framework. Obtain IT and business management approval for the targets.
- Performance data needed by the monitoring approach are collected satisfactorily and in an automated fashion, wherever feasible. Verify that the measured performance is compared to the targets at agreed-to intervals.
- There are procedures for ensuring consistency, completeness and integrity of performance monitoring source data
- There is a process to control all changes to performance monitoring data sources
- Performance targets have been defined and focus on those that provide the largest insight-to-effort ratio
- The integrity of the data collected is assessed by carrying out reconciliation and control checks at agreed-upon intervals

ME1 Monitor and Evaluate IT Performance (cont.)

Control Objective	Value Drivers	Risk Drivers
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.	• Monitoring method and approach meeting management's expectations • Enhanced decision support for IT • Alignment with the enterprise decision-making process • Transparent and reliable performance information	• Ineffective reporting on organisationwide IT process performance indicators • Business expectations and needs not met • Wrong decisions based on unreliable performance information

Test the Control Design

- Confirm that the IT process performance reports are integrated into the IT monitoring system.
- Ensure that the data in these reports are easy to understand and concise and that they meet management and end-user requirements for effective, timely decision making.
- Inspect performance reports to confirm that they appropriately cover IT objectives and outcome and performance measures and clarify cause-and-effect relationships.

Control Objective	Value Drivers	Risk Drivers
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.	• Enhanced cost-efficiency of service quality and readiness for future change • Continuous process improvement • A greater level of accountability and ownership of performance within the organisation	• Process performance weaknesses remaining and repeating themselves • Lost opportunities for improvement • Good performance not recognised, demotivating staff

Test the Control Design

- Interview process owners to confirm that target performance levels for key processes are established and validated against the industry and competition.
- Inspect performance reports for timeliness of measurement and effectiveness of comparison to the targets.
- Verify that informal feedback is obtained and used for service delivery and/or reporting improvements.
- Analyse performance reports to verify that results are consistently assessed against targets at agreed-to intervals and that relevant stakeholders receive reporting data.
- Inspect evidence of performance assessment, and determine if the assessment and analysis are complete and effective.
- For an appropriate sample, verify that causes are identified and translated into remedial actions that are assigned to someone with the appropriate authority and resource and followed up appropriately.
- Enquire whether and confirm that root causes are periodically identified across deviations and appropriately acted upon.

ME1 Monitor and Evaluate IT Performance (cont.)

Control Objective	Value Drivers	Risk Drivers
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.	• Quality reporting that meets the board's governance requirements • Performance information that can be effectively and efficiently used for strategic, managerial and day-to-day operations • Enhanced decision-making processes in responding to business needs and concerns, and a focus on process improvement opportunities • Increased satisfaction of management and the board with performance reporting	• Decisions failing to support the business needs and concerns • Senior management dissatisfied with IT performance • Disconnect between management and IT • Inability of the board and executive to direct and control key IT activities

Test the Control Design

- Enquire whether and confirm that a board and executive reporting process has been established.
- Verify that the reporting covers IT's contribution to the business by measuring achievement of IT goals, mitigation of IT risks and the usage of resources and that it is based on the performance monitoring framework (e.g., balanced scorecards, trending analysis, executive dashboards).
- Confirm that board and executive reports are based on consolidated information of IT performance measurement.
- Verify that there is a process in place to manage report versions and iterations.

ME1 Monitor and Evaluate IT Performance (cont.)

Control Objective	Value Drivers	Risk Drivers
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's proactive commitment to remedial action • Underlying performance problems resolved effectively and in a timely manner • Process performance taken seriously, and a culture of continuous improvement encouraged	• Incidents due to unresolved problems • Poor performance not acted upon, leading to further degradation • Performance measurement not taken seriously

Test the Control Design

- Enquire whether processes, policies and procedures exist to initiate, prioritise and allocate responsibility and tracking for all remedial actions. Confirm by inspecting the documentation of the approach and observing the process, where possible.
- For a sample, test whether remedial action tasks are accurately responding to the performance issue detected and that progress reviews are conducted periodically.
- Analyse historic performance reports, and verify that substandard performance trends are routinely identified and consistently escalated to senior management, including deviations from agreed-upon implementation of corrective actions.
- Search activity logs/reports for satisfactory completion of remedial action tasks determined by pre-specified outcomes, and confirm that these remedial action tasks were signed off as appropriately addressing the cause.
- Enquire whether and confirm that performance measurement training is performed.

Take the following steps to test the outcome of the control objectives:
- Interview stakeholders and assess their knowledge and awareness of key IT processes and how they are measured and monitored to ensure that the monitoring system supports the corporate performance management system.
- Review plans, policies and procedures for monitoring the performance of key IT processes to ensure that they support critical business processes.
- Determine if the IT monitoring system supports the current business strategy and facilitates effective monitoring.
- Corroborate with independent sources (stakeholders and systems-related source) that management is measuring the appropriate performance indicators.
- Review plans, policies and procedures for monitoring the performance of key IT processes for integration with the enterprise's performance management system.
- Review the documentation and communication of relationships and dependencies between key IT processes, particularly flowcharts, systems overview diagrams and dataflow diagrams.
- Review documented performance metrics with management to ensure appropriate coverage as follows:
  - Business contribution including, but not limited to, financials
  - Performance against the strategic business and IT plan
  - Risk and compliance with relevant legislation and regulations
  - Internal and external user satisfaction with service levels
  - Key IT processes, including solution and service delivery
  - Future-oriented activities, e.g., forecasting of implications related to emerging technology, reusable infrastructure, and business and IT personnel skill sets
- Review documented performance metrics to confirm that they:
  - Represent business and IT goals and objectives
  - Are based on accepted good practices
  - Focus on the most important ones
  - Are useful for internal and external comparison
  - Reflect business expectations
  - Are meaningful to IT's customers and sponsors
- Confirm that IT performance requirements are established in conjunction with business management and aligned with enterprise management's key performance metrics.
- Review appropriate approval by senior and business management of IT performance measurements and plans for communication to all process stakeholders.
- Review minutes, action lists, policies, plans and procedures related to performance measurement for evidence of regular review and update of the performance measurement approach.
- Review whether collection of performance data is covered adequately in the business requirements documentation.
- Review the data collection process and confirm that automation is considered.
- Assess the consistency, completeness and integrity of source data.
- Confirm that targets have been defined and properly signed off on by IT, senior and business management.
- Review plans, policies and procedures for organisational training to ensure skills in measurement, data collection and analysis and that the staff members adopt and promote the performance measurement culture.
- Determine if the data collected are reconciled to the source data at agreed-upon intervals.
- Inspect the measurement reports (e.g., balanced scorecard, pie charts, KPI matrices) of the enterprise and IT measurement systems, and determine if the method is integrated in the enterprise monitoring system.
- Confirm through interviews with key staff members whether the monitoring and reporting method/system is suitable and relevant for the objectives of performance measurement.
- Enquire whether and confirm that quality and completeness of output are verified. (e.g., compare actual output with expected findings and confirm results with management).
- Review the performance measurement system to determine if targets and measurement data are correct and complete.
- Enquire whether and confirm that management regularly reviews the integrity of the data quality measurements.
- Inspect performance reports for timeliness of measurement and effectiveness of comparison to the targets.
- Inspect performance reports to verify that performance results are consistently and completely assessed against targets at agreed-to intervals and that relevant stakeholders receive reporting data.
- Ensure that causes are identified and translated into remedial actions that are assigned to someone with the appropriate authority and resource and are followed up appropriately.
- Enquire whether and confirm that root causes are periodically identified across deviations and appropriately acted upon.
- Through independent sources, verify that root cause analysis does occur and results in reaction.
- Inspect that documentation exists and verify that those responsible for the underlying causes are aware of the issues.
- Confirm that senior management reports highlight key issues (positive and negative) generally relating to IT's contribution to the business and specifically to IT solution and service delivery capability and performance.
- Enquire whether and confirm that IT performance measurement is clearly linked to business outcomes and how IT supports business strategy.

- Verify that IT performance measurement is translated into business performance impacts and incorporated into standard periodic reports to the board.
- Trace results from the source to consolidated reports to assess the accuracy, completeness and reasonableness of consolidated performance reports.
- Review management reports to verify that deviations from expected performance are identified and management has committed to addressing issues (e.g., action items, management comments to recommendations, estimated resolution time frame).
- Review project documentation to confirm that remediation actions identified in senior management reports follow the organisation's change management process (e.g., AI6 *Manage change*) and that it covers elements of change management, such as project plan, appropriate approvals, progress reporting, project changes/deviation tracking, completion and sign-off.
- Inspects project documentation for remedial action tasks, and compare to the agreed-upon resolution to ensure that all monitoring deficiencies have been properly mitigated.
- Determine whether progress reviews are conducted periodically.

Take the following steps to document the impact of the control weaknesses:
- Independently benchmark the performance measurement and monitoring approach against similar organisations or appropriate international standards/recognised industry best practices.
- Corroborate performance metrics used by the enterprise with independent sources (e.g., good practice, internal and industry benchmarks).
- Benchmark the performance targets and monitoring data collection approach against similar organisations or appropriate international standards/recognised industry best practices.
- Compare actual to planned performance in all IT areas.
- Compare actual to anticipated user satisfaction with all IT areas.
- Corroborate with enterprise, IT and business management to determine if IT performance reports are useful and understandable.
- Benchmark the performance targets and monitoring data collection approach against similar organisations or appropriate international standards/recognised industry best practices.
- Assess whether senior management is satisfied with reporting on performance monitoring.

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 Objective	Value Drivers	Risk Drivers
ME2.1 Monitoring of Internal Control Framework Continuously monitor, benchmark and improve the IT control environment and control framework to meet organisational objectives.	• IT meeting its objectives for the business • Reduced impact of control failure or deficiency on the business processes • Continuous improvement of process controls with respect to industry practices • Proactive detection and resolution of control deviations • Compliance with laws and regulations	• Increased adverse impact on the organisation's operations or reputation • Control weaknesses hampering effective business process execution • Undetected malfunctioning of internal control components

Test the Control Design

- Assess whether there is executive-level support for organisational governance standards for internal control and risk management (e.g., minutes, corporate policies, interview with CEO). Verify that policies and procedures include governance for internal standards and risk management (e.g., adoption of COSO *Internal Control—Integrated Framework*, COSO *Enterprise Risk Management—Integrated Framework*, CobiT).
- Assess whether there is a continuous improvement approach to internal control monitoring (i.e., balanced scorecard, self-assessment).

Control Objective	Value Drivers	Risk Drivers
ME2.2 Supervisory Review Monitor and evaluate the efficiency and effectiveness of internal IT managerial review controls.	• Confirmation that IT processes supporting the achievement of business goals are under effective and efficient control • Contribution of reviewed results to the overall decision-making process	• Control deficiencies hampering the business processes • Inaccurate or incomplete control deficiency data, resulting in erroneous management decisions

Test the Control Design

- Confirm that the internal controls that require supervisory oversight and review are identified and consider the criticality and risk of the related IT process activities (e.g., existence of risk ranking of key processes/controls).
- Confirm that an escalation process for issues identified by supervisory reviews has been defined.
- Understand the automation of control monitoring and reporting.

ME2 Monitor and Evaluate Internal Control (cont.)

Control Objective	Value Drivers	Risk Drivers
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.	• Ability to implement preventive measures for recurring exceptions • Ability to apply corrective measures in a timely manner • Enhanced reporting to all affected parties to comply with the defined service levels • Minimised potential for compliance failures	• Control deficiencies identified not in a timely manner • Management not informed about control deficiencies • Extended time required to resolve the identified issues, thus decreasing the process performance

Test the Control Design

- Confirm that policies include establishing thresholds for acceptable levels of control exceptions and control breakdowns.
- Confirm that the escalation procedures for control exceptions have been communicated and reported to business and IT stakeholders (e.g., via the intranet, hard copy procedures). The escalation procedures should include criteria or thresholds for escalations (e.g., control exceptions less than a specific amount of impact do not need to be escalated, control exceptions greater than a specific amount of impact need immediate reporting to CIO, and control exceptions greater than a specific amount of impact require immediate reporting to the board of directors). Interview management to assess knowledge and awareness of the escalation procedures, as well as root cause analysis and reporting.
- Confirm that individuals have been assigned accountability for root cause analysis and reporting as well as exception resolution.

ME2 Monitor and Evaluate Internal Control (cont.)

Control Objective	Value Drivers	Risk Drivers
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.	• Ability to implement preventive measures for recurring exceptions • Ability to apply corrective measures in a timely manner • Enhanced reporting to all affected parties to comply with the defined service levels • Control deficiencies identified before adverse impact occurs • Proactive approach to improving service quality • Minimised potential for compliance failures	• Control deficiencies not identified in a timely manner • Management not informed about control deficiencies • Extended time required to resolve the identified issues, thus decreasing the process performance

Test the Control Design

- Review control self-assessment procedures to ensure the inclusion of relevant information such as scope, self-assessment approach, evaluation criteria, frequency of self-assessment, roles and responsibilities, and results reporting to executive business and IT stakeholders (e.g., reference internal audit standards or accepted practices in the design of self-assessments).
- Corroborate with management to determine if independent reviews of control self-assessment are performed against industry standards and best practices to ensure objectivity and to enable the sharing of internal control good practices (e.g., benchmarking against maturity model levels across similar organisations and the relevant industry).

ME2 Monitor and Evaluate Internal Control (cont.)

Control Objective	Value Drivers	Risk Drivers
ME2.5 Assurance of Internal Control Obtain, as needed, further assurance of the completeness and effectiveness of internal controls through third-party reviews.	• Identification of process control improvement opportunities, resulting in improved service to the business • Establishment and maintenance of effective internal control framework • Control skills and knowledge communicated within the organisation to increase the awareness of internal control principles and practice	• Processes not effectively controlled and failing to meet the business requirements • Objective recommendations not obtained, resulting in IT control arrangements not being optimised • Control gaps not identified • Compliance with regulatory, contractual and legal requirements not achieved

Test the Control Design

- Verify that independent control reviews, certifications or accreditations are performed periodically according to risk and business objectives along with required external skill sets (e.g., conduct an annual risk assessment and define risk areas for review).
- Verify that the review results have been reported to an appropriate management level (e.g., audit committee) and remedial action has been initiated.

ME2 Monitor and Evaluate Internal Control (cont.)

Control Objective	Value Drivers	Risk Drivers
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.	• Identification of service improvement opportunities for third parties • Confirmation of an effective internal control framework over third-party service providers • Assurance provided over the service provider's performance and compliance with internal controls	• Insufficient assurance over the service provider's control framework and control performance • Failures of mission-critical systems during operation • IT services failing to meet the service specifications • Failures and degradations of service from the provider not identified in a timely manner • Reputational damage caused by provider service performance degradation

Test the Control Design

- Confirm that internal control requirements are addressed in the policies and procedures for contracts and agreements with third parties and that appropriate provisions for rights to audit are included.
- Confirm that there is a process in place to ensure that reviews are periodically performed to access the internal controls of all third parties and that non-compliance issues are communicated.
- Confirm that policies and procedures are in place to confirm receipt of any required legal or regulatory internal control assertions from affected third-party service providers.
- Confirm that policies and procedures are in place to investigate exceptions, and obtain assurance that appropriate remedial actions have been implemented.

ME2 Monitor and Evaluate Internal Control (cont.)

Control Objective	Value Drivers	Risk Drivers
ME2.7 Remedial Actions Identify, initiate, track and implement remedial actions arising from control assessments and reporting.	• Assurance that identified control gaps are remediated as necessary • Safeguarding of continued functioning of business-critical applications • Support of the organisation's overall risk management process • Maintenance of agreed-upon service levels	• Previously identified control gaps continuing to cause problems • Malfunctioning of business-critical applications • Reputational damage caused by failure to correct service provider control deficiencies

Test the Control Design

- Confirm that procedures are established to initiate, prioritise and assign responsibility for all remedial actions, with appropriate tracking of actions.
- Confirm that there is a mechanism to detect substandard performance of the remediation and that corrective actions are identified and reviewed by management (e.g., project milestones). Confirm that continued substandard performance of the remediation is escalated to senior management for further action (e.g., project status reporting, IT steering committee minutes).
- Confirm that established procedures require remedial action tasks to be approved upon satisfactory completion against prespecified outcomes.

Take the following steps to test the outcome of the control objectives:
- Review internal control monitoring policies and procedures to ensure that they adhere to organisational governance standards, industry-accepted frameworks and industry best practices.
- Determine whether independent assessments of IT controls are required and reports on IT internal control systems are generated for management review.
- Review the independent evaluation reports (e.g., outsourced development or production activities) of the IT internal control system to determine if the proper boundaries are considered and approved by executive management.
- Review and confirm the establishment of processes and procedures to ensure that control exceptions are promptly reported, followed up and analysed.
- Confirm that corrective actions are chosen and implemented to address the control exceptions.
- Review activity logs or pertinent documentation for control exceptions, and confirm that exceptions are promptly reported, followed up, analysed, tracked and corrected.
- Confirm that periodic review is performed to ensure that the IT internal control system is current to recent business changes and the associated business and IT risks.
- Confirm that any gaps between the framework and business processes have been identified and evaluated along with appropriate recommendations. For example, ensure that business systems for operations are not maintained by IT, so established controls policies and procedures used by IT are not applied.
- Confirm that the performance of the IT control framework is regularly reviewed, evaluated, and compared to industry standards and best practices.
- Review the last control exceptions resolution progress status report to confirm that control exceptions monitoring is timely and effective.
- Review control self-assessment schedules, and select a sample of control self-assessment plans and reports to determine if control self-assessments procedures are followed for effective ongoing monitoring.
- Review a sample of the control self-assessment reports for independent review, benchmarking and remedial actions for control exceptions noted (consider ranking the significance of the control exceptions and prioritise remedial actions accordingly).
- Confirm that control self-assessment outcomes and exceptions are reported and there is a process to track control exceptions and remedial actions.
- Assess the competence of external specialists or staff members performing independent reviews for relevant IT audit experience, relevant industry knowledge and appropriate certifications/training.
- Confirm that the personnel performing the reviews are independent (e.g., review the signed confidentiality agreement).
- Review existing contracts for third-party services on IT controls, and validate that the terms and conditions cover clear scope, assignment of liability and confidentiality.
- Confirm that any significant internal control deficiencies identified are reported for immediate management attention.
- Corroborate with members of management to determine if they review the results of third-party compliance review to ensure that third parties comply with required legal, regulatory and contractual obligations.
- Select a sample of the third-party contracts and examine for specification of internal control requirements and establishment of rights to audit provision(s) as appropriate.
- Corroborate to determine if any of the following is performed: certification/accreditation review, appropriate audit engagement (e.g., SAS 70 Type II engagement) or direct audit of the service provider by IT management.
- For a sample of third parties, obtain and review internal control compliance testing reports to ensure that the third-party service providers comply with applicable laws, regulations and contractual commitments.
- Review evidence to ensure that non-compliance issues are communicated and there are remedial action plans (including time frame) in place to address the issues.
- Review the method used to prioritise remediation of control deficiencies for reasonableness.
- Review the list of remediation issues and determine whether those issues are properly prioritised (e.g., critical, high, medium and low).
- Review project scheduling tools and compare to remediation actions to confirm that the areas identified as high risk are adequately prioritised.
- Inspect the sign-offs and determine whether they occurred in a timely manner.

Take the following steps to document the impact of the control weaknesses:
- Calculate the impact on the organisation for each actual key control failure.
- Quantify the risk and likelihood to the impact on the organisation for each potential key control failure.

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 Objective	Value Drivers	Risk Drivers
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.	• Identification of good practices for dealing with laws and regulations • Improved personnel awareness for regulatory requirements • Increasing process performance and compliance with laws and regulations • Improved corporate performance	• Relevant laws or regulations overlooked, leading to non-compliance • Potential areas of financial losses and penalties not identified • Decreased customer and business partner satisfaction • Increased likelihood of disputes with customers and regulators • Increased risk to business continuity from sanctions imposed by regulators • Poor corporate operational and financial performance

Test the Control Design

- Confirm that procedures are in place to ensure that legal, regulatory and contractual obligations impacting IT are reviewed. These regulatory compliance procedures should:
  - Identify and assess the impact of the applicable legal or regulatory requirements relevant to the IT organisation
  - Update the associated IT policies and procedures affected by the legal and regulatory requirements
  - Include areas such as laws and regulations for electronic commerce, data flow, privacy, internal controls, financial reporting, industry-specific regulations, intellectual property copyright, and health and safety
  - Include the frequency of legal or regulatory requirements review (e.g., annually or when there is a new or updated legal, regulatory and contractual requirement)
- Confirm that a log of all applicable legal, regulatory and contractual requirements; their impact; and required actions are maintained and up to date.

ME3 Ensure Compliance With External Requirements (cont.)

Control Objective	Value Drivers	Risk Drivers
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.	• Support of the enterprise's compliance with applicable laws and regulations through the use of standards and methodologies • Policies regularly reviewed and aligned with the organisation's objectives • Improved personnel awareness of legal and regulatory compliance requirements • Increasing process performance in relation to compliance with laws and regulations	• Non-compliance areas not identified • Outdated compliance requirements remaining in effect • Policies failing to meet the enterprise's compliance needs • Personnel unaware of procedures and practices to comply with legal and regulatory requirements

Test the Control Design

- Confirm that there are procedures and practices to ensure compliance with legal, regulatory and contractual requirements.
- Confirm that appropriate functions are included (e.g., legal department, production, accounting, HR).

Control Objective	Value Drivers	Risk Drivers
ME3.3 Evaluation of Compliance With External Requirements Confirm compliance of IT policies, standards, procedures and methodologies with legal and regulatory requirements.	• Good practices for dealing with laws and regulations incorporated effectively into enterprise arrangements • Increasing process performance and compliance with laws and regulations • Deviations identified to support timely corrective action	• Financial losses and penalties • Decreased customer and business partner satisfaction • Non-compliance incidents not identified, adversely impacting the enterprise's performance and reputation • Increased likelihood of disputes

Test the Control Design

- Review the IT organisation policies, standards and procedures and confirm their regular and timely update to address any non-compliance (legal and regulatory) gaps identified.

ME3 Ensure Compliance With External Requirements (cont.)

Control Objective	Value Drivers	Risk Drivers
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.	• Confirmation of the enterprise's compliance with applicable laws and regulations through the use of standards and methodologies • Good practices identified for dealing with laws and regulations effectively incorporated into enterprise arrangements • Increasing process performance in relation to compliance with applicable laws and regulations • Confirmation that deviations from compliance requirements are identified and corrected in a timely manner	• Failure to report non-compliance incidents, adversely impacting the enterprise's performance and reputation • Increased likelihood of disputes • Areas of non-compliance not identified and reported • Corrective actions not initiated in a timely manner, adversely impacting the overall performance of the organisation

Test the Control Design

- Review from process owners evidence of regular confirmation of compliance with applicable laws, regulations and contractual commitments (i.e., final report and letter from regulators acknowledging the completion of their review).
- Review that processes are in place to track and execute internal and external reviews to ensure that there is adequate planning and resource allocation to assist/complete reviews (e.g., inventory of regulatory requirements, scheduling of internal compliance reviews, scheduling of resources required to assist reviews).
- Enquire whether procedures are in place to regularly assess levels of compliance with legal and regulatory requirements by independent parties.
- Review policies and procedures to ensure that contracts with third-party service providers require regular confirmation of compliance (e.g., receipt of assertions) with applicable laws, regulations and contractual commitments.
- Confirm that a process to monitor and report on incidents of non-compliance is implemented that includes, where necessary, further investigation of the root cause of incidents taking place.

ME3 Ensure Compliance With External Requirements (cont.)

Control Objective	Value Drivers	Risk Drivers
ME3.5 Integrated Reporting Integrate IT reporting on legal, regulatory and contractual requirements with similar output from other business functions.	• Facilitated corporate reporting on compliance issues • Enabling of timely detection of control gaps where they are interfering with other business functions • Support of the organisation's standards and methodologies in establishing effective compliance arrangements • Reduced overall compliance risk facing the enterprise	• Increased enterprise non-compliance exposure • Other business functions unaware of compliance requirements and status related to IT processes • Failure to integrate IT-related compliance issues into overall reporting, resulting in erroneous strategic decision making by enterprise management

Test the Control Design

- Enquire whether and confirm that:
  - Requirements are co-ordinated for corporate reporting on legal and regulatory compliance, including the requirement to retain any historical information
  - IT compliance reporting conforms with corporate reporting requirements, such as distribution, frequency, scope, content and format, to ensure reporting consistency and completeness

Take the following steps to test the outcome of the control objectives:
- Trace specific compliance requirements from recognition and documentation through the procedures to prevent and detect non-compliance. Interview and assess relevant staff members to confirm that they are aware of legal, regulatory and contractual requirements that have been identified.
- Review evidence or a log of applicable laws, regulations and standards and the company's compliance status from internal and independent counsel's input. For non-compliance areas, identify management remedial actions to address the requirements.
- Confirm that coverage, procedures and practices for compliance are regularly reviewed by internal and external experts (e.g., security audits, SAS 70s).
- Confirm that advice from appropriate third parties is obtained as required.
- Review IT processes documentation for evidence of periodic legal and regulatory compliance review, and ensure that the documents are updated where appropriate.
- Enquire if recurring patterns of compliance failures are looked for and their cause evaluated on a regular basis (e.g., determine if changes to policies, standards, procedures, processes and activities are implemented as a result of the evaluations).
- Review compliance assessment reports on legal and regulatory requirements performed by independent internal or external parties to ensure that regular reviews take place.
- Review a sample of third-party contracts to determine if there are provisions to require regular confirmation of compliance with applicable laws, regulations and contractual commitments.
- Select a sample of third-party service providers and obtain evidence of their assertions of compliance to determine if they comply with the contractual requirement of regular confirmation of compliance.
- Review findings from third-party compliance reporting as well as from non-compliance investigation and resolution to determine if operating effectiveness deficiencies are addressed.
- Confirm that standards for IT compliance reporting conform with the agreed-upon format, including scope, content and format, required to ensure consistency and completeness (e.g., review agreement procedures)
- Review compliance reports to ensure that the IT compliance assessment results were incorporated and presented consistently with similar reports from other business functions.

Take the following steps to document the impact of the control weaknesses:
- Identify and quantify the cost of fines and other penalties levied against the enterprise as a result of non-compliance.
- Quantify the risk and likelihood of non-compliance with regulatory requirements (e.g., "Statement of the Securities and Exchange Commission Concerning Financial Penalties," US Securities and Exchange Commission [SEC], 2006), to assist in the understanding of the impact on the enterprise.

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 Objective	Value Drivers	Risk Drivers
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.	• IT decisions in line with the enterprise's strategies and objectives • A consistent approach for a governance framework achieved and aligned with the enterprise approach • Processes overseen effectively and transparently • Compliance with legal and regulatory requirements confirmed • Board requirements for governance likely to be met	• Ineffective responsibilities and accountabilities established for IT processes • The IT portfolio failing to support the enterprise's objectives and strategies • Remedial actions to maintain and improve IT process effectiveness and efficiency not identified or implemented • Controls not operating as expected

Test the Control Design

- Enquire whether and confirm that:
  - An agreed-upon process exists to align the IT governance framework with the overall enterprise governance and control environment
  - The framework is based on a comprehensive IT process and control model and defines leadership, unambiguous accountability, roles and responsibilities, information requirements, organisational structures, and practices to avoid breakdown in internal control and oversight
  - Appropriate management governance structures exist, such as the IT strategy committee, IT steering committee, technology council, IT architecture review board and IT audit committee. Verify that terms of reference exist for each of these.
  - The IT governance framework focuses on strategic alignment, value delivery, resource management, risk management and performance measurement
  - A process exists to measure and evaluate delivery of IT's strategies and objectives, and to aggregate all IT governance issues and remedial actions into a consolidated management repository or tracking mechanism
  - Unambigous responsibilities for IT risk management have been established
  - IT governance status and issues are reported to the corporate governance oversight body

ME4 Provide IT Governance (cont.)

Control Objective	Value Drivers	Risk Drivers
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.	• IT more responsive to the enterprise's objectives • IT resources helping to facilitate the business goals in an efficient and effective manner • IT capabilities enabling opportunities for the business strategy • Efficient allocation and management of IT investments	• Ineffective allocation and management of IT investments • IT failing to support the enterprise's objectives • Strategic IT planning not aligned with the overall corporate strategy • IT directions not defined and not supporting business goals

Test the Control Design

- Inspect IT strategy documentation and assess whether it supports the direction provided by the board/senior management. It should reflect business strategies and IT's appropriate alignment with business operations.
- Determine whether the IT strategic planning process includes involvement from business operations and demonstrates alignment with business strategies and objectives.
- Review the IT strategy documents and assess whether they include the role of IT, IT guiding principles from business maxims, how IT monitors the business impact of the IT infrastructure and applications portfolio, and the potential contribution of IT to the overall business strategy (e.g., evaluating, post-implementation, benefits delivered by IT projects).

ME4 Provide IT Governance (cont.)

Control Objective	Value Drivers	Risk Drivers
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.	• Cost-efficient delivery of solutions and services • Optimised use of IT resources • Business needs supported efficiently • Increasing support for use of IT by enterprise stakeholders • Increased value contribution of IT to business objectives • Reliable and accurate picture of costs and likely benefits	• Misdirected IT investments • Value not obtained from the IT assets and services • Decreasing customer satisfaction • Increasing costs for IT investments and operations • Lack of alignment between the business objectives and the IT architecture • Expected benefits not realised

Test the Control Design

- Confirm that there is co-responsibility between the business and IT for all IT investments.
- Inspect documentation that identifies how IT delivers against the strategy. It should include delivering on time and within budget, with appropriate functionality and the intended benefits.
- Determine whether there is a process to regularly identify and evaluate ways to increase IT value contribution whilst managing business and executive expectations with respect to emerging technology (i.e., steering committee meetings).
- Determine whether there is a partnership between the business and the IT providers, with shared responsibility for sourcing decisions.
- Determine whether IT is aware of (or has documented) business expectations for IT value (i.e., time-to-market, cost and time management, partnering success) and that IT perceives the value of IT consistently.
- Determine whether there is an effective process to ensure that IT and business architectures are designed to drive maximum value.
- Determine whether there is an effective process in place to adjust IT investments based on a balance of risk, cost and benefit with budgets that are acceptable and take into account return and competitive aspects of IT investments.
- Inspect IT documentation to assess whether the business has set expectations for the content of IT deliverables, including meeting business requirements; flexibility to adopt future requirements; throughput and response times; ease of use; security; and the integrity, accuracy and currency of information.
- Determine whether there is an effective IT portfolio management process that is being evaluated on a regular basis to optimise value in relation to costs and that results in (for the business) competitive advantage, elapsed time for order/service fulfilment, customer satisfaction, employee productivity and profitability.
- Review the results of management's monitoring of the IT budget and investment planning to ensure that it remains realistic and integrated into the overall financial plan (this may include compliance with regulatory requirements).
- Determine that the IT asset portfolio management process effectively manages and reports on the actual costs and the ROI.

ME4 Provide IT Governance (cont.)

Control Objective	Value Drivers	Risk Drivers
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.	• Efficient and effective prioritisation and utilisation of IT resources • IT costs optimised • Increased likelihood of benefit realisation • IT planning supported and optimised • Readiness for future charge	• Fragmented, inefficient infrastructures • Insufficient capabilities, skills and resources to achieve desired goals • Strategic objectives not achieved • Inappropriate priorities used for allocation of resources

Test the Control Design

- Confirm through questioning of management that a high-level direction for sourcing and use of IT resources is in place.
- Review minutes of meetings with high-level directors to determine effectiveness of these direction activities.
- Enquire whether and confirm that suitable IT resources, skills and infrastructure are available to meet strategic objectives and that policies are in place to enable continued availability.
- Enquire whether and confirm that IT infrastructures are provided that facilitate the creation and sharing of business information at optimal cost.
- Review that policies, procedures and processes are in place for resource management, and verify that they are operating effectively to:
  – Optimise and balance overall IT investments and use of resources between sustaining and growing the enterprise
  – Capitalise on information and knowledge resources
  – Establish business priorities so that resources are allocated to enable effective IT performance
- Independently develop and estimate optimal balance of overall IT investments and use of resources, and compare with actual findings.
- Trace items through the IT infrastructures, and determine whether creation and sharing of information is facilitated effectively.
- Enquire whether and confirm that critical roles are allocated and defined for driving maximum value from IT with appropriate staffing and resources.
- Review the defined roles, and ensure that they are effectively allocated and executed.
- Enquire whether and confirm that procedures for capability assessments are in place and regularly performed to ensure an ability to support the business strategy.
- Reperform capability assessments and compare to defined business strategies.

ME4 Provide IT Governance (cont.)

Control Objective	Value Drivers	Risk Drivers
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.	• Risks identified before they materialise • Increased awareness of risk exposures • Clear accountability and responsibility for managing critical risks • Effective approach for managing IT risks • IT risk profile aligned with management's expectations • Minimised potential for compliance failures	• Risks identified or managed ineffectively • Increased expenses and costs incurred to manage unanticipated risks • Critical IT applications and services failure • Lack of ownership of IT risks

Test the Control Design

- Enquire whether and confirm that:
  - Based on information from management, such as IT risk exposures, risk management measures and associated costs, the board defines, regularly re-evaluates and communicates the enterprise's risk appetite
  - Management reviews the outcome of the evaluation of the risk of IT activities, to confirm that the total risk exposure does not exceed the defined risk appetite, considering mitigating controls in place, and oversees the implementation of additional mitigating controls to reduce the overall risk exposure as needed
  - A process exists to include IT risk management issues in IT governance status and issues reporting and to provide transparency of IT risks to all stakeholders

ME4 Provide IT Governance (cont.)

Control Objective	Value Drivers	Risk Drivers
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.	• Increased process performance • Areas of improvement identified • IT objectives and strategies being and remaining in line with the enterprise's strategy • Processes overseen effectively and transparently • Timely and effective management reporting enabled	• Performance gaps not identified in a timely manner • Decreased stakeholder confidence • Service deviations and degradations not recognised and addressed, resulting in failure to deliver business requirements • Service performance failures causing legal and regulatory compliance exposures

Test the Control Design

- Enquire whether and confirm that:
  - The IT scorecard performance measures are properly aligned with the business scorecard measures and accepted by the business
  - Management assesses and accepts the effectiveness of the processes and the accuracy and completeness of the deliverables to measure and report IT performance in relation to achievement of the strategic IT objectives. Verify that status reports include the extent to which planned objectives have been achieved, deliverables obtained and performance targets met.
  - The board evaluates the appropriateness of management's corrective actions for significant performance problems and provides direction to rectify organisational or systemic causes as necessary

ME4 Provide IT Governance (cont.)

Control Objective	Value Drivers	Risk Drivers
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.	• Opportunities for service improvements identified • Gaps detected in a timely manner • Reliable assurance of effective governance, risk management, and internal control mechanisms and procedures • Assurance to the board and executive management that governance is working effectively	• Reputational damage through failure to detect or prevent service performance degradation • Ineffective IT governance, risk management and internal control arrangements • Unethical behaviours adopted and accepted

Test the Control Design

- Enquire whether and confirm that an audit committee has been established with a mandate to consider what the significant risks are; assess how they are identified, evaluated and managed; commission IT and security audits; and rigorously follow up closure of subsequent recommendations.
- Interview the audit committee and assess its knowledge and awareness of its responsibilities. Determine whether the established audit committee is operating effectively.
- Enquire whether and confirm that independent reviews, certifications or accreditations of compliance with IT policies, standards and procedures have been obtained. Physically inspect for adequacy the documents produced by the independent reviews.

Take the following steps to test the outcome of the control objectives:
- Review board/senior management meeting minutes to determine whether business direction is provided over enterprise use of IT resources and capabilities.
- Review the enterprise leadership and organisational structures related to the use of IT resources to determine their appropriateness in relation to the overall enterprise and the completeness of their coverage of oversight and management of IT resources.
- Identify the process model being used to establish and support IT governance, and assess its adequacy and effectiveness of application.
- Review IT strategic planning minutes to verify that IT and business goals and objectives are aligned.
- Confirm that there are business sponsors designated to have direct active involvement in and accountability for all major IT-enabled investments.
- Review plans for IT services and compare with the business strategy to assess that the direction allows IT to provide optimal support.
- Confirm through interviews with those responsible for IT strategy that it is integrating well with overall business goals.
- Assess whether the goals and objectives of the business and IT are clearly communicated to relevant parties and that appropriate mediation exists and is functioning effectively (e.g., technology plans).
- Assess whether an IT steering committee drives business alignment by ensuring that IT strategy is aligned with business strategy and that supporting strategies and plans are consistent and integrated.
- Determine whether there is a process for executive management to regularly review IT governance reports to determine whether IT strategic issues and actions to resolve them are reported. Such reports should include progress against strategic plans, key service performance measures, and significant risk assessment and mitigation aspects.
- Identify and assess the extent of independent assurance provided to the enterprise in relation to the establishment and effectiveness of IT governance arrangements.

Take the following steps to document the impact of the control weaknesses:
- Quantify the impact of failures of IT to support new business initiatives or critical business services.
- Identify IT-related incidents and issues that attract media attention and comment (e.g., major failed projects, compliance violations, security failures).

Page intentionally left blank

APPENDIX VI—APPLICATION CONTROL (AC)

APPENDIX VI—APPLICATION CONTROL (AC)

PROCESS ASSURANCE STEPS

AC1 Source Data Preparation and Authorisation

Control Objective	Value Drivers	Risk Drivers
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. Minimise errors and omissions through good input form design. Detect errors and irregularities so they can be reported and corrected.	• Data integrity • Standardised and authorised transaction documentation • Improved application performance • Accuracy of transaction data	• Compromised integrity of critical data • Unauthorised and/or erroneous transactions • Processing inefficiencies and rework

Test the Control Design

- Ensure that the design of the system provides for the identification and management of authorisation levels.
- Enquire whether and confirm that the design of the system provides for the use of preapproved authorisation lists and related signatures for use in determining that documents have been appropriately authorised.
- Assess whether source documents and/or input screens are designed with predetermined coding, choices, etc., to encourage timely completion and minimise the potential for error.
- Enquire whether and confirm that the design of the system encourages review of the forms for completeness and authorisation and identifies situations where attempts to process incomplete and/or unauthorised documents occur.
- Enquire whether and confirm that, once identified, the system is designed to track and report upon incomplete and/or unauthorised documents that are rejected and returned to the owner for correction.

Test the Outcome of the Control Objective

- Verify, through inspection of authorisation lists, that authorisation levels are properly defined for each group of transactions. Observe that authorisation levels are properly applied.
- Inspect and observe creation and documentation of data preparation procedures, and enquire whether and confirm that procedures are understood and the correct source media are used.
- Where required by procedures, observe whether and ensure that adequate segregation of duties between originator and approver exists.
- Inspect documents, trace transactions through the process and, where possible, use automated evidence collection, including sample data, embedded audit modules or CAATs, to trace transactions to verify that authorisation access controls are effective.
- Enquire whether and confirm that a list of authorised personnel and their signatures is maintained by the appropriate departments. Where possible, use automated evidence collection, including sample data, embedded audit modules or CAATs, to trace transactions to verify that the list of authorised personnel is effectively designed to allow/restrict personnel to enter data.
- Inspect the list of authorised personnel and other documentation, and observe processes and procedures to verify that the processes and procedures used to maintain the list are timely and effective. Select a sample of employees and assess whether their authorisation levels are commensurate with their roles and responsibilities.
- Enquire whether and confirm that all source documents include standard components such as predetermined input codes and default values to reduce errors, record transaction time and date to provide for monitoring, and capture authorisation information to ensure validity.
- Where possible, use automated evidence collection, including sample data, embedded audit modules or CAATs, to select transactions for subsequent verification of the use of standard components that improve accuracy and provide evidence of authorisation.

AC1 Source Data Preparation and Authorisation (cont.)

Test the Outcome of the Control Objective (*cont.*)
• Enquire whether and confirm that, during data entry, source documents are reviewed; incomplete, unsigned or inappropriately authorised documents are returned to originators for correction and are logged; and logs are periodically reviewed to verify that corrected documents are returned by originators in a timely fashion. Inspect source documents and review logs and other documents to verify that incomplete documents are effectively detected and completed by originators in a timely manner. • Review source document forms and verify if they are usable, facilitate error prevention, and enable speedy and efficient preparation.

AC2 Source Data Collection and Entry

Control Objective	Value Drivers	Risk Drivers
Ensure 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.	• Accurate data entry and efficient processing • Errors detected in a timely manner • Sensitive transaction data secured	• Processing inefficiencies due to incomplete data entry • Compromised integrity of critical data • Access control violations • Data entry errors undetected

Test the Control Design

- Enquire whether and confirm that criteria for timeliness, completeness and accuracy of source documents are defined and communicated.
- Enquire whether and confirm that documented procedures for the correction of errors, out-of-balance conditions and entry of overrides exist. Ensure that the procedures include mechanisms for timely follow-up, correction, approval and resubmission. Assess procedures for factors such as descriptions of error messages and override mechanisms.
- Enquire whether and confirm that policies and processes are established to establish criteria for the identification of classes of critical transactions that require pre-numbered source documents or other unique methods of identifying source data.
- Enquire whether and confirm that there are policies and procedures in place to determine document retention policies. Factors to consider in assessing the document retention policy include criticality of the transaction, form of the source data, method of retention, location of retention, time period for retention, compliance and regulatory requirements.
- For each major group of transactions, enquire whether and confirm there is documentation of criteria to define authorisation for input, editing, acceptance, rejection and override.
- Inspect documentation of policies and procedures to ensure that criteria for timeliness, completeness and accuracy are appropriately represented.

Test the Outcome of the Control Objective

- Enquire whether and confirm that critical source documents are prenumbered and out-of-sequence numbers are identified and taken into account.
- Enquire whether and confirm that error messages are generated in a timely manner, transactions are not processed unless errors are corrected or appropriately overridden, errors that cannot be corrected immediately are logged and valid transaction processing continues, and error logs are reviewed and acted upon within a specified and reasonable period of time.
- Enquire whether and confirm that reports on errors and out-of-balance conditions are reviewed by appropriate personnel; all errors are identified, corrected and checked within a reasonable period of time; and errors are reported until corrected.
- For a sample of transaction flows, enquire whether and confirm that retention of source documents is defined and applied in relation to established criteria for source document retention.
- Select a set of critical transactions and:
  - Compare the actual state of access controls over transaction input, editing, acceptance, etc., with established criteria, policies or procedures.
  - Inspect whether critical source documents are prenumbered or that other unique methods of identifying source data are used.
  - Inspect documentation or walk-through transactions to identify those personnel who can input, edit, authorise, accept and reject transactions and override errors.
  - Take a sample of transactions within this set for a specific period, and inspect the source documents for those transactions. Verify that all appropriate source documents are available.
- Identify and review out-of-sequence numbers, gaps and duplicates using automated tools (CAATs).
- Inspect documents, trace transactions through the process and, where possible, use automated evidence collection, including sample data, embedded audit modules or CAATs, to trace transactions to verify that authorisation controls are effective and that sufficient evidence is reliably recorded and reviewed.

AC2 Source Data Collection and Entry (cont.)

Test the Outcome of the Control Objective (*cont.*)
• Inspect documents, trace transactions through the process and, where possible, use automated evidence collection, including sample data, embedded audit modules or CAATs, to trace transactions to verify that timely error messages, transaction process restrictions and error logs are generated, applied and reviewed effectively. • Inspect error and out-of-balance reports, error corrections, and other documents to verify that errors and out-of-balance conditions are effectively reviewed, corrected, checked and reported until corrected.

AC3 Accuracy, Completeness and Authenticity Checks

Control Objective	Value Drivers	Risk Drivers
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.	• Data processing errors efficiently remediated • Data accuracy, completeness and validity maintained during processing • Uninterrupted transaction processing • Segregation of duties for data entry and processing	• Processing inefficiencies and reworks due to incomplete, invalid or inaccurate data entry • Compromised integrity of critical data • Data entry errors undetected • Unauthorised data entry

Test the Control Design

- Enquire whether and confirm that policies and procedures exist for the handling of transactions that fail edit and validation checks.
- Enquire whether and confirm that processes and procedures are established for the segregation of duties for entry, modification and approval of transaction data as well as for validation rules. Factors to consider in the assessment of segregation of duties policies include criticality of the transaction system and methods for the enforcement of segregation of duties.
- Enquire whether and confirm that validation criteria and parameters on input data are periodically reviewed, confirmed and updated in a timely, appropriate and authorised manner.
- For important or critical systems, inspect the data input design to ensure that the authorisation controls allow only appropriately authorised persons to input or modify data.
- Obtain functional description and design information on data input controls. Inspect the functionality and design for appropriate controls. Examples of controls include the presence of sequence, limit, range, validity, reasonableness, table look-ups, existence, key verification, check digit, completeness (e.g., total monetary amount, total items, total documents, hash totals), duplication, logical relationship checks and time edits.
- Obtain functional description and design information on data input authorisation controls. Inspect the functionality and design for the presence of authorisation checks.
- Obtain functional description and design information on transaction data entry. Inspect the functionality and design for the presence of timely and complete checks and error messages. If possible, observe transaction data entry.
- Obtain functional description and design information on transaction data validation.

Test the Outcome of the Control Objective

- Inspect error and out-of-balance reports, error corrections, and other documents to verify that errors and out-of-balance conditions are effectively reviewed, corrected, checked and reported until corrected.
- Inspect error corrections, out-of-balance conditions, entry overrides and other documents to verify that the procedures are followed.
- Select a sample of input source data of source documents. Using inspection, CAATs, or other automated evidence collection and assessment tools, validate that input data are a complete and accurate representation of underlying source documents.
- Select a sample of source data input processes. Enquire whether and confirm that mechanisms are in place to ensure that the source data input processes have been performed in line with established criteria for timeliness, completeness and accuracy
- Enquire whether and confirm that transactions failing edit and validation routines are subject to appropriate follow-up until they are remediated.

AC4 Processing Integrity and Validity

Control Objective	Value Drivers	Risk Drivers
Maintain the integrity and validity of data throughout the processing cycle. Ensure that detection of erroneous transactions does not disrupt processing of valid transactions.	• Processing errors detected in a timely manner • Ability to investigate problems	• Insufficient evidence of errors or misuse • Data entry errors undetected • Unauthorised data processing

Test the Control Design

- Enquire whether and confirm that transaction processing takes place only after appropriate authorisation is given.
- Review the documentation of the tools and applications to verify they are applicable and suitable for the task. Where appropriate for critical transactions, review the code to confirm that controls in the tools and applications operate as designed. Reprocess a representative sample to verify that automated tools operate as intended.
- Obtain functional description and design information on data input controls. Inspect the functionality and design for the presence of sequence and duplication errors, referential integrity checks, control, and hash totals. With searching tools, identify cases where errors were identified erroneously and cases where errors were not detected.
- Inspect the functional description and design information on transaction data entry to verify whether transactions failing edit and validation routines are posted to suspense files. Verify whether suspense files are correctly and consistently produced and that users are informed of transactions posted to suspense accounts. Verify that processing of transactions is not delayed by data entry or transaction authorisation errors. Use automated evidence collection, including sample data, base cases (prepared transactions with an expected outcome), embedded audit modules or CAATS, to trace transactions to verify that transactions are processed effectively, valid transactions are processed without interruption from invalid transactions and erroneous transactions are reported.
- Analyse a representative sample of error transactions on suspense accounts and files, and verify that transactions failing validation routines are checked until remediation. Verify whether suspense accounts and files for transactions failing validation routines contain only recent errors, confirming that older ones have been appropriately remediated.
- Enquire whether and confirm that jobs sequence is indicated to IT operations. Enquire whether and confirm that jobs provide adequate instructions to the job scheduling system so data are not inappropriately added, changed or lost during processing. Inspect source documents, trace transactions through the process and, where possible, use automated evidence collection, including sample data, embedded audit modules or CAATS, to trace transactions to verify that production job scheduling software is used effectively so that jobs run in the correct sequence and provide adequate instructions to the systems.
- Enquire whether and confirm that every transaction is assigned a unique and sequential number or identifier (e.g., index, date, time). Inspect documents, trace transactions through the process and, where possible, use automated evidence collection, including sample data, embedded audit modules or CAATS, to trace transactions to verify that there are no duplicates for transactions that require unique IDs and there are no gaps that need to be sequentially numbered.
- Enquire whether and confirm that the audit trail of transactions processed is maintained. Inspect the audit trail and other documents to verify that the audit trail is designed effectively. Use automated evidence collection, including sample data, embedded audit modules or CAATS to trace transactions to verify that the audit trail is maintained effectively. Verify that before and after images are maintained and periodically reviewed by appropriate personnel.
- Enquire whether and confirm that the transaction audit trail is maintained and periodically reviewed for unusual activity. Verify that the review is done by a supervisor who does not perform data entry. Inspect the audit trail, transactions (or batches), reviews and other documents; trace transactions through the process; and, where possible, use automated evidence collection, including sample data, embedded audit modules or CAATS, verify that periodic review and maintenance of the audit trail effectively detects unusual activity and supervisor reviews are effective to verify the validity of adjustments, overrides and high-value transactions in a timely manner.
- Enquire whether and confirm that appropriate tools are used and maintenance of thresholds complies with the security requirements. Enquire whether and confirm that a supervisor periodically reviews system output and thresholds. Use automated evidence collection, including sample data, embedded audit modules or CAATS, to trace transactions to verify that the tools work as designed.
- Enquire whether and confirm that utilities are used, where possible, to automatically maintain the integrity of data during unexpected interruptions in data processing. Inspect the audit trail and other documents, plans, policies and procedures to verify that system capabilities are effectively designed to automatically maintain data integrity. Review the records of actual interruptions involving data integrity issues and verify that appropriate tools were used effectively.

AC4 Processing Integrity and Validity (cont.)

Testing the Control Design (*cont.*)

- Enquire whether and confirm that adjustments, overrides and high-value transactions are promptly reviewed in detail for appropriateness by a supervisor who does not perform data entry. Inspect the audit trail, other documents, plans, policies and procedures to verify that adjustments, overrides and high-value transactions are designed effectively to be promptly reviewed in detail. Inspect the audit trail, transactions (or batches), reviews and other documents; trace transactions through the process; and, where possible, use automated evidence collection, including sample data, embedded audit modules or CAATS, to verify that supervisor reviews are effective to ensure the validity of adjustments, overrides and high-value transactions in a timely manner.
- Enquire whether and confirm that reconciliation of file totals is performed on a routine basis and that out-of-balance conditions are reported. Inspect reconciliations and other documents and trace transactions through the process to verify that reconciliations effectively determine whether file totals match or the out-of-balance condition is reported to the appropriate personnel.

Test the Outcome of the Control Objective

- For a sample application, enquire whether and confirm that segregation of duties is in place. Verify whether segregation of duties is implemented for entry, modification and approval of transaction data as well as for validation rules.
- For a sample of critical transactions processes, test whether access controls prevent unauthorised data entry. With searching tools, identify cases where unauthorised personnel are able to input or modify data.
- For a sample of transaction systems, verify whether suspense accounts and suspense files for transactions failing edit and validation routines contain only recent errors. Confirm that older failing transactions have been appropriately remediated.
- For a sample of transactions, verify that data entry is not delayed by invalid transactions.
- For highly critical transactions, set up a test system that operates like the live system. Enter different types of errors.
- Verify whether error detection and reporting are timely and complete and if they provide sufficient information to correct the transaction.
- For highly critical transactions, set up a test system that operates like the live system. Process transactions in the test system to ensure that valid transactions are processed appropriately and in a timely fashion.
- Ensure that errors are reported appropriately and in a timely fashion.
- Inspect error messages upon data entry or online processing.
- Ensure that error messages are appropriate for the transaction flow. Examples of appropriate attributes of messages include understandability, immediacy and visibility.
- Determine whether transactions failing edit and validation routines are posted to suspense files.
- Verify whether suspense files are correctly and consistently produced.
- Verify whether the user is informed of transactions posted to suspense accounts.
- Take a sample of data input transactions. Use appropriate automated analysis and search tools to identify cases where errors were identified erroneously and cases where errors were not detected.
- Use automated evidence collection, including sample data, embedded audit modules or CAATS, to verify that valid transactions are processed without interruption. Inspect whether and confirm that invalid transactions are reported in a timely manner.

AC5 Output Review, Reconciliation and Error Handling

Control Objective	Value Drivers	Risk Drivers
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.	• Sensitive data output protected • Complete and error-free processing results delivered to the right recipient • Errors detected in a timely manner	• Sensitive transaction data delivered to wrong recipient • Compromised data confidentiality • Inefficient transaction processing • Transaction data output errors undetected

Test the Control Design

- Review design criteria and confirm that they require the use of integrity-based control processes, such as the use of control totals in header and/or trailer records and the balancing of output back to control totals produced by the system.
- Enquire whether and confirm that detected out-of-balance conditions are reported, reports have been designed into the system and procedures have been developed to ensure that reports are provided to the appropriate level of management.
- Enquire whether and confirm that procedures require that out-of-balance conditions and other abnormalities require prompt investigation and reporting.
- Review the documentation and ensure that procedures specify that periodic inventories be taken of key sensitive documents and differences be investigated.
- Enquire whether and confirm that procedures have been designed to ensure that the completeness and accuracy of application output are validated prior to the output being used for subsequent processing, including use in end-user processing.
- Enquire whether and confirm that procedures have been developed to ensure that output is reviewed for reasonableness, accuracy or other criteria established by the process owner prior to use.
- Assess whether procedures have been defined that require the logging of potential errors and their resolution prior to distribution of the reports.

Test the Outcome of the Control Objective

- Enquire whether and confirm that control totals are properly implemented in header and/or trailer records of output to balance back to control totals produced by the system.
- Enquire whether and confirm that detected out-of-balance conditions are reported to the appropriate level of management. Inspect out-of-balance reports. Where possible, use automated evidence collection to look for control total errors and verify that they were acted upon correctly and in a timely manner.
- Enquire whether and confirm that physical inventories of sensitive outputs are taken at appropriate intervals. Ensure that they are compared to inventory records and that any differences are acted upon. Confirm that audit trails are created to account for all exceptions and rejections of sensitive output documents. Inspect a representative sample of audit trails using automated evidence collection, if possible, to identify exceptions and verify whether they have been detected and action has been taken. Take a physical inventory sample, and compare it to the associated audit trails to verify that detection operates effectively.
- Obtain a list of all electronic outputs that are reused in end-user applications. Verify that the electronic output is tested for completeness and accuracy before the output is reused and reprocessed. Select a representative sample of electronic output, and trace selected documents through the process to ensure that completeness and accuracy are verified before other operations are performed. Reperform completeness and accuracy tests to validate that they are effective.
- Enquire whether and confirm that output is reviewed for reasonableness and accuracy. Select a representative sample of output reports and test the reasonableness and accuracy of the output. Verify that potential errors are reported and centrally logged. Select a sample of representative transactions and verify that errors are identified and addressed in a timely manner. Inspect error logs to verify that errors are effectively addressed in a timely manner.
- Enquire whether and confirm that sensitive information is defined, agreed upon by the process owner and treated appropriately. This may include labelling sensitive application output and, where required, sending sensitive output to special access-controlled output devices. For a sample of sensitive data, search output files and confirm that they are properly labelled. Review the distribution methods of sensitive information and the access control mechanisms of sensitive output devices. Verify that the mechanisms correctly enforce pre-established access rights.

AC6 Transaction Authentication and Integrity

Control Objective	Value Drivers	Risk Drivers
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.	• Straight-through processing • Confidence in validity and authenticity of transactions • Errors and misuse prevented	• Erroneous and/or unauthorised transactions • Transaction errors undetected • Inefficiencies and rework

Test the Control Design

- Enquire whether and confirm that a process has been designed to ensure that, for critical transactions, appropriate agreements have been made with counterparties that include communication and transaction presentation standards, responsibilities, authentication and security requirements.
- Enquire whether and confirm that systems are designed to incorporate appropriate mechanisms for integrity, authenticity and non-repudiation, such as adoption of a secure standard or one that is independently verified.
- Enquire whether and confirm that systems are designed to incorporate industry standard output tagging to identify authenticated information.
- Inspect manuals and documentation for critical applications to confirm that design specifications require that input be appropriately verified for authenticity.
- Enquire whether and confirm that systems are designed to identify transactions received from other processing applications, and analyse that information to determine authenticity of origin of the information and whether integrity of content was maintained during transmission.
- Obtain and inspect agreements made with counterparties for critical transactions, and ensure that the agreements specify requirements for communication and transaction presentation standards, responsibilities, authentication and security requirements.
- Select a sample of counterparty agreements for critical transactions and verify that they are complete.
- Select a sample of authentication failures to verify that the counterparty agreements operate effectively.
- Review documentation and perform a walk-through to identify applications that are critical for transaction authenticity, integrity and non-repudiation. For these applications, enquire whether and confirm that an appropriate mechanism for integrity, authenticity and non-repudiation is adopted (i.e., a secure standard or one that is independently verified).
- Inspect application manuals and documentation for critical applications to confirm that specifications and the design state that output is appropriately tagged with authentication information.
- Perform a walk-through of the code of a sample of applications to confirm that this specification and design are applied. Verify that these specifications have been tested with good result.
- Select a representative sample of transactions, and verify that authenticity and integrity information is correctly carried forward throughout the processing cycle.
- Review error logs for transactions that failed authentication, and verify the cause.

Test the Outcome of the Control Objective

- Perform a walk-through of the code of a sample of applications to confirm that specifications for authenticity have been applied. Verify that these specifications have been tested with good result.
- Review error logs for transactions that failed authentication, and verify the cause.

Page intentionally left blank

Appendix VII—Maturity Model for Internal Control

APPENDIX VII—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

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 the 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 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. While 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 responsibilities 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 best 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 VIII—IT Scoping

APPENDIX VIII—IT SCOPING

1. Define the Initiative.
Define the purpose of the initiative, the business objective and the expected value to be returned. Document the enterprise areas addressed and impacted. List the success factors, compliance requirements, potential risks and project closure criteria. Establish how changes to these project drivers and outcomes will be handled.

Step	Activities	Deliverables
Step 1.1 Define objectives. Identify the primary objectives and goals of the initiative. Develop the value proposition and indicate how the objectives support and enhance the goals of the enterprise.	• Identify reasons and objectives for undertaking the project and review with management. • Research and document key issues and concerns. • Learn from similar projects that have been undertaken. • Identify and obtain relevant documents. • Identify the expected outcome and deliverables of the initiative (high level). • Identify the competitive landscape.	• Documented business values • Documented objectives of the IT initiative • Documented expected outcomes
Step 1.2 Define boundaries. Define the IT project and its boundaries, what is included and what is excluded. Identify the organisational units, business activities and processes that are included, and those that are excluded from the project scope.	• Identify key activities, business units, organisational entities, operations, etc., to be included within the scope of the project. • Identify and document items that are normally within the scope of such projects but that are to be excluded. • Identify any scope issues, such as partially owned entities, foreign jurisdictions or exclusions. • Ensure that the scope is sufficient to ensure that the results obtained will meet the objectives and expected deliverables. • Establish liaison with affected entities to ensure co-ordination.	• Documented scope of the IT initiative • Documented scope of boundary issues and their treatment • Communication of the boundaries with key stakeholders
Step 1.3 Define standards. Identify standards, reference frameworks, policies and/or contracts with which the initiative needs to comply. Standards may include industry requirements, regulatory standards and entity policies. Identify indicators for measuring, and establish key success factors for achieving compliance.	• Identify contractual, legislative, regulatory, industry or other standards to which the entity and the project must comply. • Identify any standards or frameworks that the project/initiative should consider. • Document success factors to enable, and key metrics to evidence, compliance with standards.	• Documented standards that will be used in undertaking the project • Documented key success factors and metrics for use in assessing project results
Step 1.4 Define risks. Identify and assess risks associated with the project, including business risks as well as project risks. The degree of risk assessment and mitigation depends on the project's size, value delivered and impact.	• Identify potential reasons for failure or delay of the initiative in meeting objectives. • Identify important scenarios that may endanger the initiative's objectives, as well as the negative impacts this initiative may have on other enterprise objectives. • Identify the significance of risks and likelihood of occurrence. • Create plans to manage and mitigate the risks.	• Documented risk assessment of the IT initiative • Risk mitigation plan (as needed) and estimated costs
Step 1.5 Define change process. Identify internal and external factors that could cause changes to the project, and define how changes will be made to the project's objectives, scope, risks and success factors.	• Identify and analyse internal and external factors that could cause changes to the project. • Define and document the process and procedures for authorising, accepting and communicating changes to the drivers and outcomes. • Identify appropriate tools and techniques to manage the change process.	• Change process description • Change management guidance, including the use of tools and techniques

Step	Activities	Deliverables
Step 1.6 Define success. Identify the conditions that must exist for the project to be considered complete, including the specific activities, tasks and deliverables required to complete the project. Define the exit criteria of the initiative (i.e., the conditions that determine if the objectives have been achieved).	• Identify post-project acceptance activities. • Identify evidence required to indicate that the project deliverables have been provided and accepted by the project owner and by those taking responsibility for the ongoing activities the project may create.	• Evidence (metrics, quality criteria, etc.) required to indicate that the project has been successfully completed • Evidence that post-completion activities have been identified and provided to appropriate organisational units
Step 1.7 Define resources. Identify the resources required to successfully complete the initiative, including people, technology, funding and skills.	• Define the number and level (skills) of resources needed to achieve the objectives of the initiative. • Assess the need for technology and equipment to support the initiative.	• Resource model • Resource cost plan
Step 1.8 Define deliverables. Define the specific deliverables that are to be produced during the initiative.	• Identify the external deliverables that will result from the initiative. • Create an illustrative sample deliverable.	• List of project deliverables • Sample of selected deliverables

2. Plan the initiative.
Define the deliverables in detail. Based on that, identify the resources, support and accountabilities required to produce the deliverables. Obtain approval, set priorities within the initiative, activate resources and develop a communication plan so that the initiative can be stage-gated.

Step	Activities	Deliverables
Step 2.1 Obtain executive support. Identify and appoint the appropriate project sponsor for the initiative.	• Determine the suitability of potential sponsors. • Assess the availability of potential sponsors to fulfil the requirements. • Develop executive presentation material based on project objectives and benefits.	• Initiative sponsor/owner • Completed project documentation and charter
Step 2.2 Finalise resource requirements. Acquire the necessary funding and resources as defined in the resource model.	• Review the expected resource model and cost plan. • Prepare a detailed acquisition timeline. • Prepare a detailed calendar-based project budget, including resource consumption/use and funding requirements.	• Updated resource model • Detailed resource acquisition timeline • Detailed project budget
Step 2.3 Define organisation for the initiative. Define and implement the organisational structure required to make the initiative successful. This will include leadership, staffing, key sponsor, etc., and may include a project management office.	• Document roles and responsibilities. • Define leadership expectations. • Create and establish the organisation structure. • Initially populate the organisation with key personnel. • Create position descriptions, roles and responsibilities.	• Organisation model • Reporting authority • Roles and responsibilities
Step 2.4 Define timeline. Define the specific timeline for the initiative to be completed to meet stated goals and objectives given the expected resources and deliverables defined for the initiative. Include key milestones and identify the critical path.	• Review goals and objectives and the expected resource model. • Based on the review, define key milestones for deliverables and major initiative checkpoints with project sponsors. • Prepare a high-level timing diagram, and identify potential critical path and dependent activities. • Prepare Gantt charts for each major phase of the subproject, including critical and slack path analysis, skill requirements, and resource plans. • Ensure that timing will meet critical external reporting, financing and other deadlines within the business cycle. • Define ongoing status reporting within the project and to key external stakeholders and affected staff members.	• Documented timelines integrated with the resource planning information • Project timeline document indicating: - Activities and tasks - Activity dependence - Major milestone dates - Major project checkpoints - Key deliverable dates - Status and reporting dates - Business activities and other key dates • Defined communications documents

Step	Activities	Deliverables
Step 2.5 Define approach and methodology. Determine the methodologies to be used and develop detailed plans, complete with phases, subphases, activities and tasks, to enable the project to successfully meet its objectives.	• Develop project phases and subphases, each with objectives, activities and deliverables. • Determine the approach and methodologies to be used and the information to be obtained. • Develop detailed work plans for each phase, subphase and activity.	• Detailed project plan
Step 2.6 Create communication plan. Design a plan to communicate information about the initiative, manage expectations and support the objectives of the initiative throughout its life cycle. Consider the key milestones and different audiences.	• Communicate project status, resource plan and costs (as appropriate). • Communicate the status of the risk management plan. • Communicate changes in project goals and objectives. • Communicate project progress.	• Documented communication plan, including time line and key milestones

Page intentionally left blank

Appendix IX—
CobiT and Related Products

APPENDIX IX—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 and measure performance
- 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 *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. The second edition is in development at the time of this writing.
- COBIT *Security Baseline, 2nd Edition*—Focuses on essential steps for implementing information security within the enterprise. The second edition is in final 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 CMMI® for Development V1.2 With COBIT 4.0*
  - *COBIT Mapping: Mapping of ISO/IEC 17799:2000 With COBIT, 2nd Edition*
  - *COBIT Mapping: Mapping of ISO/IEC 17799:2005 With COBIT 4.0*
  - *COBIT Mapping: Mapping of ITIL With COBIT 4.0*
  - *COBIT Mapping: Mapping of PMBOK With COBIT 4.0*
  - *COBIT Mapping: Mapping of PRINCE2 With COBIT 4.0*
  - *COBIT Mapping: Mapping of SEI's CMM for Software With COBIT 4.0*
- *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*.

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*