2ND EDITION

COBIT® CONTROL PRACTICES

GUIDANCE TO ACHIEVE CONTROL OBJECTIVES FOR SUCCESSFUL IT GOVERNANCE

Control Practices

Control Objectives

Value Drivers

Risk Drivers

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

Disclaimer
The IT Governance Institute (the 'Owner') and the author have designed and created this publication, titled *COBIT® Control Practices: Guidance to Achieve Control Objectives for Successful IT Governance, 2nd Edition* (the "Work"), primarily as an educational resource for chief information officers (CIOs), senior management, IT management and control professionals. The Owner makes no claim that use of any of the Work will assure a successful outcome. The Work should not be considered inclusive of all 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, controls professionals should apply their own professional judgement to the specific control circumstances presented by the particular systems or information technology environment.

Disclosure

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

ISBN 1-933284-87-0
COBIT® Control Practices: Guidance to Achieve Control Objectives for Successful IT Governance, 2nd Edition
Printed in the United States of America

ACKNOWLEDGEMENTS

IT Governance Institute wishes to recognise:

Workshop Participants and Expert Reviewers

Mark Adler, CISA, CISM, CIA, CISSP, Allstate Ins. Co., USA
Peter Andrews, CISA, CITP, MCMI, PJA Consulting, UK
Georges Ataya, CISA, CISM, CISSP, MSCS, PBA, Solvay Business School, Belgium
Gary Austin, CISA, CIA, CISSP, CGFM, KPMG LLP, USA
Gary S. Baker, CA, Deloitte & Touche, Canada
David H. Barnett, CISSP, CISM, Applera Corp., USA
Christine Bellino, CPA, CITP, Jefferson Wells, USA
John W. Beveridge, CISA, CISM, CFE, CGFM, CQA, Massachusetts Office of the State Auditor, USA
Alan Boardman, CISA, CISM, CA, CISSP, Fox IT, UK
David Bonewell, CISA, CISSP-ISSEP, Accomac Consulting LLC, USA
Dirk Bruyndonckx, CISA, CISM, KPMG Advisory, Belgium
Don Canilglia, CISA, CISM, USA
Luis A. Capua, CISM, Sindicatura General de la Nación, Argentina
Boyd Carter, PMP, Elegantsolutions.ca, Canada
Sean V. Casey, CISA, CPA, USA
Sushil Chatterji, Edutech, Singapore
Edward Chavannes, CISA, CISSP, 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
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 Eduardo Fabius, CISA, Republica AFAP S.A., Uruguay
Urs Fischer, CISA, CIA, CPA (Swiss), Swiss Life, Switzerland
Christopher Fox, ACA, PricewaterhouseCoopers, USA
Bob Frelinger, CISA, Sun Microsystems Inc., USA
Zhiwei Fu, Ph.D, Fannie Mae, USA
Monique Garsoux, Dexia Bank, Belgium
Edson Gin, CISA, CFE, SSCP, USA
Sauvik Ghosh, CISA, CIA, CISSP, CPA, Ernst & Young LLP, USA
Guy Groner, CISA, CIA, CISSP, USA
Erik Guldentops, CISA, CISM, University of Antwerp Management School, Belgium
Gary Hardy, IT Winners, South Africa
Jimmy Heschl, CISA, CISM, KPMG, Austria
Benjamin K. Hsaio, CISA, Federal Deposit Insurance Corp., USA
Tom Hughes, Acumen Alliance, Australia
Monica Jain, CSQA, Covansys Corp., US
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

Workshop Participants and Expert Reviewers (*cont.*)
Linda Kostic, CISA, CPA, USA
John W. Lainhart IV, CISA, CISM, IBM, USA
Philip Le Grand, Capita Education Services, UK
Elsa K. Lee, CISA, CISM, CSQA, AdvanSoft International Inc., USA
Kenny K. Lee, CISA, CISSP, Countrywide SMART Governance, USA
Debbie Lew, CISA, Ernst & Young LLP, USA
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
Ed O'Donnell, Ph.D., CPA, University of Kansas, USA
Sue Owen, Department of Veterans Affairs, Australia
Robert G. Parker, CISA, CA, CMC, FCA, Robert G. Parker Consulting, Canada
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
Roger Southgate, CISA, CISM, FCCA, CubeIT Management Ltd., UK
Paula Spinner, CSC, USA
Mark Stanley, CISA, Toyota Financial Services, USA
Dirk E. Steuperaert, CISA, PricewaterhouseCoopers, Belgium
Robert E. Stroud, CA Inc., USA
Scott L. Summers, Ph.D., Brigham Young University, USA
Lance M. Turcato, CISA, CISM, CPA, City of Phoenix IT Audit Division, USA
Wim Van Grembergen, Ph.D., University of Antwerp Management School, Belgium
Johan Van Grieken, CISA, Deloitte, Belgium
Greet Volders, Voquals NV, Belgium
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

ACKNOWLEDGEMENTS

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

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

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, Republica AFAP SA, Uruguay
Urs Fischer, CISA, CIA, CPA, Swiss Life, Switzerland
Erik Guldentops, CISA, CISM, University of Antwerp Management School, Belgium
Gary Hardy, IT Winners, South Africa
Jimmy Heschl, CISA, CISM, KPMG, Austria
Debbie A. Lew, CISA, Ernst & Young LLP, USA
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 Assurance and IGM Financial, Canada, Chair
Roland Bader, F. Hoffmann-La Roche AG, Switzerland
Linda Betz, IBM, USA
Jean-Pierre Corniou, EDS Consulting Services, France
Rob Clyde, CISM, Symantec, USA
Richard Granger, NHS Connecting for Health, UK
Howard Schmidt, CISM, R&H Security Consulting LLC, USA
Alex Siow Yuen Khong, StarHub Ltd., Singapore
Amit Yoran, Yoran Associates, USA

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

TABLE OF CONTENTS

Page intentionally left blank

INTRODUCTION TO THIS GUIDE

INTRODUCTION TO THIS GUIDE

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 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

The COBIT IT processes, business requirements and control objectives define what needs to be done to implement an effective control structure to improve IT performance and address IT solution and service delivery risks.

COBIT, 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—Describe 34 IT processes covering the IT responsibility areas from beginning to end
- Control objectives—Provide generic good practice management objectives for IT processes
- Management guidelines—Offer tools to help assign responsibility, measure performance, and benchmark and address gaps in capability
- Maturity models—Provide profiles of IT processes describing possible current and future states

COBIT Control Practices: Guidance to Achieve Control Objectives for Successful IT Governance, 2nd Edition, provides guidance on the risks to be avoided and value to be gained from implementing a control objective, and instruction on how to implement the objective. Control practices are strongly recommended for use with the *IT Governance Implementation Guide: Using COBIT® and Val IT™, 2nd Edition*.

COBIT Control Practices offers the more detailed guidance needed by management, service providers, end users and control professionals and helps them with justifying and designing the specific controls needed. The material in the second edition consists of control practice statements expressed as action-oriented implementation steps derived from the first publication released in 2004 and now aligned with COBIT 4.1.

The control practices provide the how, why and what to implement for each control objective to improve IT performance and/or address IT solution and service delivery risks. This material is of use to:
- Management, service providers, end users and control professionals who need to justify and design or improve specific controls
- Assurance professionals who may be asked for their opinions regarding proposed implementations or necessary improvements

By providing guidance on why controls are needed and what good practices will help toward meeting specific control objectives, *COBIT Control Practices, 2nd Edition*, helps ensure that solutions put forward are more likely to be completely and successfully implemented.

The elements of the *COBIT Control Practices, 2nd Edition*, are:
- Value and risk statements—Provide guidance to help articulate why it is worthwhile to implement the control objective. The value statements provide examples of the business benefits that can be derived from achieving the control objective, while the risk statements provide examples of the risks that can be mitigated. They help both assurance professionals and IT governance implementers provide a justification and a business case for implementing control improvements and for substantiating the risk of controls not being adequately addressed.
- Control practices—For the process controls (generic process-level control objectives), the application controls and for the specific control objectives in each IT process

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

COBIT assumes the design and implementation of automated application controls to be the responsibility of IT, covered in the Acquire and Implement domain. The operational management and control responsibility for application controls is not with IT, but with the business process owner. Hence, the responsibility for application controls is an end-to-end joint responsibility between business and IT, with the business being responsible for properly defining functional and control requirements and IT being responsible for automating, implementing and establishing controls to maintain the integrity of applications. The application controls are identified by ACn, for application control number.

In addition, three generic control practices are suggested that apply to the implementation of each control objective. They are:
- **Approach**—Design the control approach for achieving this control objective and define and maintain the set of control practices that implement this design.
- **Accountability and responsibility**—Define and assign accountability and responsibility for the control objective as a whole, and responsibility for the different control practices (see RACI chart). Make sure personnel have the right skills and necessary resources to execute these responsibilities.
- **Communication and understanding**—Ensure that the manner in which the control practices implement the control objective is communicated and understood.

A complete set of generic and specific control practices provides one control approach consisting of all the steps that are necessary and sufficient for achieving the control objective. They provide high-level guidance, at a level below the control objective for assessing actual performance and for considering potential improvements. However, they may not be at a sufficient level of detail for implementation and further guidance may need to be obtained from specific relevant standards and best practices such as ITIL, ISO/IEC 17799 and PRINCE2.

The control practices can be used to compare to current capabilities and also to guide the design of improvements.

In summary, each control practice:
- Is a non-prescriptive control design for achieving the control objective
- Describes a set of necessary and sufficient steps to achieve a control objective
- Is action-oriented
- Is relevant to the purpose of the control objective
- Considers the inputs, activities and outputs of the process
- Supports establishment of clear roles and responsibility

PC — Process Control

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

CONTROL PRACTICES

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

Control Practices

1. Define and communicate process goals and objectives for the effective execution of each IT process.
2. Link process goals and objectives to business goals.
3. Ensure that process goals are defined in a SMARRT manner.
4. Define process outputs and measurable quality targets to assess output quality. Use personal targets to motivate positive results.

PC2 Process Ownership

Control Objective	Value Drivers	Risk Drivers
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.	• Processes operating smoothly and reliably • Processes interacting with each other effectively • Process problems and issues identified and resolved • Processes continually improved	• Processes performing unreliably • Processes not working together effectively • Gaps in process coverage likely • Process errors not rectified

Control Practices

1. Assign an owner for each IT process such that responsibility is clear.
2. 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, measurements of process performance and the identification of improvement opportunities.
3. Ensure that the process owner has sufficient authority to implement, drive and improve the process.
4. Establish process ownership and accountability for the process's end deliverables, and ensure that ownership and accountabilities are accepted. Assign and communicate unambiguous roles and responsibilities for efficient execution of the key activities and their documentation. Record roles, responsibilities and accountabilities in job descriptions, and ensure that assigned roles are accepted.

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

Control Practices

1. Base all processes on standardised good practice.
2. Develop standards and templates for all processes.
3. Ensure that the process is documented in a consistent manner and in a form that helps staff members perform their function.
4. Design the process to provide reliability as well as flexibility appropriate for the type of process.
5. Monitor, review and continuously improve the process.

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

Control Practices

1. Define the key activities and end deliverables of the process, and establish relevant process documentation, such as policies, plans and procedures.
2. Review achievement of individual objectives through regular job performance appraisals to assess:
   - Whether roles and responsibilities are executed as defined
   - Whether process-related activities are performed in line with goals and objectives
   - The individual's contribution to the quality of the process's end deliverables

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

Control Practices

1. Define and communicate rules on how all IT process-related documentation (e.g., policies, plans, procedures, guidelines, instructions, methodologies) that drives an IT process is developed, documented, reviewed, maintained, approved, stored, used for training and communicated.
2. Assign responsibilities for developing, maintaining, storing and communicating process-related documentation. Review and sign off on process policies, plans and procedures, where needed.
3. Ensure that the IT process-related documentation is accessible, correct, understood and up to date.
4. Create IT process-related documentation so it can be put into practice and support the repeatability of the process.

PC6 Process Performance Improvement

Control Objective	Value Drivers	Risk Drivers
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.	• Process costs optimised • Processes nimble and responsive to business needs	• Process outcomes and deliverables not in line with overall IT and business objectives • Processes too costly • Processes slow to react to business needs

Control Practices

1. Establish a set of key metrics with a high insight-to-effort ratio that enables measurement of the achievement of process goals, resource utilisation, output quality and throughput time to support improvement of the process performance and outcome.
2. Define relationships between outcome and performance metrics, and integrate them into the enterprise's performance management system (e.g., balanced scorecard), where appropriate.
3. Establish specific targets for process goals and performance drivers. Define how the data are obtained, including mechanisms to facilitate process measurement (e.g., automated and integrated tools, templates).
4. Compare actual measurement to the target and take action for significant deviations.
5. For key processes, compare process performance and process outcomes against internal and external benchmarks, and consider the result of the analysis for process improvement.

Page intentionally left blank

PO — Plan and Organise

CONTROL PRACTICES

PO1 Define a Strategic IT Plan

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 service level agreements (SLAs). Accountability for achieving the benefits and controlling the costs should be clearly assigned and monitored. Establish fair, transparent, repeatable and comparable evaluation of business cases, including financial worth, the risk of not delivering a capability and the risk of not realising the expected benefits.	• 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

Control Practices

1. Define a committee, supported by a formal charter and containing both IT and business unit leadership, with the objective of directing IT-enabled investment programmes, IT services and IT assets.
2. Ensure that the management activities of the IT-enabled investment programmes, IT service and IT assets use a formal process that requires business cases that include cost-benefit analysis, analysis of alignment with business strategy, risk assessments, SLAs for IT services and the impact to the current IT portfolio.
3. Ensure that the management activities of the IT-enabled investment programmes include a process that:
   - Monitors the development and delivery of IT components of investment programmes
   - Requires reviews of IT service delivery against equitable and enforceable SLAs
   - Monitors deviations in terms of cost, timing and functionality
4. Ensure that accountability for value delivery, i.e., the achievement of business benefits through the use of IT, is clearly assigned at an appropriate level.

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

Control Practices

1. Ensure that IT informs enterprise management and key stakeholders on the current technology environment, possible future trends and value opportunities for the business.
2. Ensure that enterprise management and key stakeholders discuss with IT management future business directions and enterprise goals to collaborate and develop a common understanding of the potential for IT to enable business goals.
3. Ensure that IT management contributes to business strategy planning and identifies capabilities available to support enterprise goals and other opportunities to contribute to business value.
4. Make the scope of the IT strategic and planning initiatives enterprisewide such that they address, document and consider all business and support activities.
5. Ensure current and future business and IT alignment by:
   - Technology creating opportunities that the business can turn into enterprise benefits
   - Involving IT management in the development of enterprise goals to recognise opportunities and current capability limitations
6. Align business imperatives and priorities with IT capabilities to establish enterprise priorities for inclusion in the IT strategic plan.
7. In conjunction with business representatives, document a prioritised list of business products, services and processes that are critically dependent on IT.

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

Control Practices

1. Capture and report feedback from IT, organisation management and key stakeholders on the current solutions and services. Considerations include, but are not limited to, strengths and weaknesses, functionality, degree of business automation, stability, complexity, development requirements, technology alignment and direction, support and maintenance requirements, costs, and external parties' (including business partners and vendors) input.
2. Ensure that IT management is apprised on a timely basis of changes in the enterprise's mission, goals and objectives, and that such changes initiate a review of the IT strategic and tactical plans and, where warranted, changes thereto.
3. Periodically compare IT's current state against the requirements of the IT strategic plan. The outcome of the evaluation includes, but is not restricted to, current requirements, current delivery to requirements, barriers to achieving requirements, and the steps and costs required to remove restrictions.
4. Consider the results of the assessment of the current performance in the strategic planning process.
5. Use internal, well-understood and reliable industry, technology or other benchmarks and good practices to assess existing solutions, services 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

Control Practices

1. Establish a process to translate business strategy, business expectations, and current and future IT capabilities into an IT strategic plan.
2. Ensure that IT has established a process to identify, document and adequately address organisational changes, technology evolution, regulatory requirements, business process re-engineering, staffing, in- and outsourcing opportunities, etc., in the planning process.
3. Define roles and responsibilities of the stakeholders involved in the strategic planning process.
4. Develop IT capabilities to support the business requirements and contribute to expected benefits as included in the enterprise's strategic plan.
5. Identify and document the implications on the business strategy in terms of risk and cost of the required IT capabilities. Resolve negative implications appropriately in co-ordination with the business.
6. Define and document the IT goals and objectives necessary to cost-efficiently:
   - Achieve the benefits and manage the risks of the capabilities required of IT
   - Establish the current and future performance required to respond to business expectations
   - Provide transparency on capabilities delivered by IT and their contribution to strategic objectives
7. Translate the business-derived IT objectives into outcome measures represented by metrics (what) and targets (how much) that can be related to business benefits. Obtain appropriate stakeholder approval.
8. Formally approve and communicate the IT strategic plan and ensure that it is clearly understood by those who need to translate it into budgets, tactical plans, sourcing and acquisition strategies, processes, and organisational structures.

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

Control Practices

1. Translate the approved IT strategic plan into tactical plans.
2. Ensure that the process of developing tactical plans allows for considerations to update strategic IT plans.
3. Ensure that the content of the tactical plans includes clearly stated project definitions for all programmes, project time frames and deliverables, required resources, and business benefits to be monitored.
4. Explicitly state goal and performance indicators, goals risk assessment results, and related risk mitigation plans within the IT tactical plans.
5. Base the planning and elaboration of the IT-enabled investment programmes, IT projects, resources utilisation and monitoring techniques on the detailed tactical plan.
6. Determine that formal and comprehensive periodic review and change management processes exist to ensure that any changes made to the organisation's mission and objectives are reflected in the IT tactical plans.
7. Use a methodology for a formal review of IT strategic and tactical plans to optimise current and future investments and strategies, in terms of the use of scarce resources, implementation alternatives, funding methods and timing.

PO1 Define a Strategic IT Plan (cont.)

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

Control Practices

1. Based on strategic and tactical IT plans, ensure that the business and IT are involved in identifying and defining IT-enabled investment programmes, IT services, assets and related IT projects.
2. Develop and promulgate prioritisation schemes relating prioritisation criteria to business goals and technical requirements. Project prioritisation may be modified due to the availability of scarce resources, implementation alternatives, funding methods, risks, and timing of competing or complementary projects.
3. Evaluate IT-enabled investment programmes, IT services and assets against prioritisation criteria to establish and update the portfolio of IT-enabled investment programmes. Determine how the portfolio supports the achievement of measurable business outcomes.
4. Translate the selected programmes and related projects into required effort, resources and funding, and obtain approval from the business.
5. Translate the programmes into clearly defined projects with required resources and funding.
6. Communicate projects that will be delayed, postponed or not continued so that business and IT management can use resources in an efficient and effective manner.
7. Obtain the required authority to launch the approved projects within the selected programmes.

PO2 Define the Information Architecture

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

Control Practices

1. Establish and maintain the information architecture model in the context of the entire organisation, documented in an understandable manner for business and IT management.
2. Develop the information architecture model consistent with the organisation's strategy and the strategic and tactical IT plans.
3. Check the information architecture model regularly for adequacy regarding flexibility, functionality, cost-effectiveness, security, failure resiliency, compliance and user satisfaction, and update the model accordingly.

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

Control Practices

1. Ensure that a data dictionary exists that is used to control and co-ordinate definitions and usage of reliable and relevant data consistent with the enterprise information model.
2. Establish and maintain data syntax guidelines that are valid throughout the organisation.
3. Verify the effectiveness of the enterprise data dictionary by identifying reductions in data redundancy and data incompatibility throughout the organisation.
4. Ensure that the business and IT agree upon data syntax rules, data validation rules and business rules.
5. Ensure that metadata in a data dictionary are sufficiently detailed to communicate syntax in an integrated manner across applications.
6. Implement data dictionary management software to manage and maintain the organisation's data dictionary and data syntax rules.
7. Implement a data quality programme to increase data integrity, standardisation, consistency, one-time data entry and storage, and to reduce flaws.

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

Control Practices

1. Create a classification scheme that defines attributes for data classification, such as data ownership, definition of security levels (confidentiality, integrity and availability), a brief description of data retention and destruction requirements.
2. Define data classification levels for each of the defined attributes (e.g., for confidentiality: public, internal, confidential).
3. Identify business owners accountable for information (data owners).
4. Ensure that the data owner classifies all information using the defined scheme and levels. Classification covers the whole life cycle of information from creation to disposal. Where an asset has been assessed as having a certain classification, any component inherits the same classification.
5. Make owners understand the consequences of the classification, and balance security needs against cost considerations and other business requirements considering the value of the assets they own.
6. Ensure that information and data are labelled, handled, protected and otherwise secured in a manner consistent with the data classification categories.

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

Control Practices

1. Define, in collaboration with business management, the required integrity and consistency criteria.
2. Implement procedures to manage and maintain data integrity and consistency throughout the complete data process and life cycle (e.g., input, processing, output, migration, extraction, archiving).
3. Implement a data quality programme to ensure data integrity and consistency through regular validation.

PO3 Determine Technological Direction

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

Control Practices

1. Perform a strengths, weaknessess, opportunities and threats (SWOT) analysis of all current critical and significant IT assets on a regular basis.
2. Follow up on market evolutions and relevant emerging technologies.
3. Identify the latest developments in IT that could have an impact on the success of the business.
4. Establish the appropriate technological risk appetite (e.g., pioneer, leader, early adopter, follower).
5. Identify what is needed in terms of technological directions for business systems architecture, migration strategies and contingency aspects of infrastructure components.

Control Objective	Value Drivers	Risk Drivers
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.	• 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	• 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

Control Practices

1. Create a technology infrastructure plan based on the IT strategic and tactical plans and technology direction, which includes factors such as consistent integrated technologies, business systems architecture and contingency aspects of infrastructure components, and directions for acquisition of IT assets.
2. Perform ongoing assessments of the current vs. planned information systems, resulting in a migration strategy or road map to achieve the future state.
3. Include transitional and other costs, complexity, technical risks, future flexibility, value, and product/vendor sustainability in the technology infrastructure plan.
4. Identify changes in the competitive environment, economies of scale for information systems staffing and investments, and improved interoperability of platforms and applications in the technology infrastructure plan.

PO3 Determine Technological Direction (cont.)

Control Objective	Value Drivers	Risk Drivers
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.	• 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	• 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

Control Practices

1. Ensure that adequately skilled staff members within the IT department routinely monitor technological developments, competitor activities, infrastructure issues, legal requirements and regulatory environment changes, and provide relevant information to senior management. Consult third-party experts to obtain views and confirm findings and proposals of internal staff.
2. Ascertain that the IT department maintains membership in vendor user groups, subscribes to technical journals and maintains a research budget.
3. Evaluate new technologies in the context of their potential contribution to the realisation of broader business goals and targets using established criteria, e.g., ROI, or ability to achieve market leadership.
4. Ensure that the organisation's legal counsel monitors legal and regulatory conditions in all relevant locations and informs the IT steering committee of any changes that may impact the technology infrastructure plan.

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

Control Practices

1. Ensure that corporate technology standards are approved by the IT architecture board and communicated throughout the organisation by using a technology forum.
2. Ensure that management establishes and maintains an approved list of vendors and system components that conform with the technological infrastructure plan and technology standards.
3. Establish a process to prevent the acquisition of non-conforming systems or applications.
4. Put technology guidelines in place to effectively support the organisation's technological solutions.
5. Put in place monitoring and benchmarking processes, such as measuring non-compliance to technology standards, to ensure compliance to the standards.
6. Update technology standards as part of a periodic review of the technological infrastructure plan. Ensure that all stakeholders are involved in the development and approval of migration strategies and change plans, taking into consideration impacts on personnel and operations.
7. Align the information systems department's recruiting and training practices with the technology standards.

PO3 Determine Technological Direction (cont.)

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

Control Practices

1. Establish an IT architecture board to provide architecture guidelines and advice on their application.
2. Agree on and formally document the role and authority of the IT architecture board. Establish that the document includes the overall IT architecture design and the alignment with the information architecture.
3. Put a process in place to monitor and benchmark the effect on business strategy and identify instances of non-compliance to technology standards.
4. Ensure that the IT architecture board meets regularly and meeting minutes are taken that include actions, assignments of responsible parties, time lines and tasks.

PO4 Define the IT Processes, Organisation and Relationships

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

Control Practices

1. Identify IT processes required to realise the IT strategic plan.
2. Define and implement a framework to enable the definition and follow-up of process goals, measures, controls and maturity.
3. Define relationships and touchpoints (e.g., inputs/outputs) amongst the IT processes, enterprise portfolio management and business processes.

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

Control Practices

1. Define the scope, objectives, membership, roles, responsibilities, etc., of the IT strategy committee.
2. Ensure that the IT strategy committee is composed of board and non-board members with appropriate expertise in the organisation's dependency on IT and opportunities provided by IT.
3. Ensure that the IT strategy committee meets on a regular basis to address strategic issues, including major investment decisions, raised by the board of directors or the organisation.
4. Ascertain that the IT strategy committee reports 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

Control Practices

1. Ensure that an IT steering committee exists that reports to an appropriate level of senior management and includes representation from the executive level, key business operations areas, IT and key business support areas such as finance, risk management, compliance, human resources, legal and internal audit.
2. Ensure that the IT steering committee includes a key sponsor at the executive level.
3. Ensure that the role and authority of the IT steering committee are agreed upon and formally documented.
4. Ensure that the IT steering committee meets regularly, with an appropriate and monitored frequency.
5. Determine that the responsibilities for the committee include at least:
   - Determination of prioritisation of IT-enabled investment programmes in line with the enterprise's business strategy and priorities
   - Tracking of status of projects and resolution of resource conflict
   - Monitoring of service levels and service improvements
6. Ensure that the IT steering committee approves the high-level control requirements, such as consideration of key performance indicators and balanced scorecards in relation to IT, and monitors controls compliance.

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 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

Control Practices

1. Determine 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.
2. Define and fund the IT function in such a way that individual user group departments cannot exert undue influence over the IT function and undermine the priorities agreed upon by the IT steering committee.
3. Ensure that the IT function is 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 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 • Inflexiblity of IT to changes in business needs

Control Practices

1. Perform periodic reviews of the impact of organisational change as it affects the overall organisation and the structure of the IT function itself.
2. Determine that the IT organisation has flexible resource arrangements to support changing business needs, such as the use of external contractors and flexible third-party service arrangements.

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

Control Practices

1. Formalise the skills, experience, authority, responsibility and accountability for each IT task. Update the IT task descriptions when IT tasks change.
2. Assign all IT tasks to one or more roles, and assign roles to IT personnel.
3. Allocate accountabilities and responsibilities to roles rather than to organisational positions to support the execution of the role. Allocate roles to organisational positions and allocate organisational positions to individuals.
4. Inform IT personnel about their roles and any changes to their roles.
5. Ensure that line managers periodically confirm the accuracy of the role descriptions for their team members.
6. Develop the role description to outline key goals and objectives, which include SMARRT measures, for use in the staff performance evaluation process.
7. Ensure that role descriptions for staff members across the organisation specifically identify responsibilities regarding information systems, internal control and security.
8. Ensure that management initiates regular training and awareness campaigns to reinforce staff knowledge of roles. This may be supplemented with occasional assessments of understanding and compliance.
9. Require all employees to comply with enterprisewide (e.g., corporate) and applicable department policies related to internal control, security and confidentiality.

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

Control Practices

1. Ensure that the QA function's reporting line is such that it can operate with adequate independence and report its findings objectively.
2. Ensure that the role of the QA function includes:
   - 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 system development life cycle), standards and procedures
   - Adopting and aligning with QA best practices and standards
3. Ensure that the staffing levels and skills for the QA function are commensurate with the size of the organisation and the QA function's responsibilities. Skills include those related to quality assurance, IT, controls, processes and communication.
4. Encourage senior management's sponsorship and active support of the QA function.
5. Define and document a process for identifying, escalating and resolving issues identified to the QA process.
6. Ensure that the QA function reports 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

Control Practices

1. Encourage senior management to establish an organisationwide, adequately staffed risk management and information security function with overall accountability for risk management and information security. 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.
2. Formalise and document roles and responsibilities for the risk management and information security function. Allocate these responsibilities to appropriately skilled and experienced staff and, in the case of information security, under the direction of an information security officer.
3. Regularly assess the resource requirements in relation to risk management and information security. Assess whether appropriate resources are provided to meet the needs of the business.
4. Put a process in place to obtain senior management guidance concerning the enterprise's risk profile and acceptance of significant residual risks.

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

Control Practices

1. Provide policies and guidelines to ensure appropriate and consistent enterprisewide classification of data.
2. Define, maintain and provide appropriate tools, techniques and guidelines to provide effective security and controls over information assets in collaboration with the owner.
3. Create and maintain an inventory of information assets (systems and data) that includes a listing of owners, custodians and asset classifications. Include assets that are outsourced and those for which ownership should stay within the organisation.

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

Control Practices

1. Ensure that the level of supervision is commensurate with the skills of the individuals being supervised and the risks and criticality of the task being performed.
2. Define and document the process for escalating issues that are identified through supervisory processes.
3. Ensure that supervisory activities include using key performance indicators related to department operations, staff performance appraisals and other methods to provide effective supervision.
4. Assess individuals with responsibility for supervision regarding their effectiveness in this area.

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

Control Practices

1. Establish standards that enforce appropriate segregation of duties. Periodically review and update the standards.
2. Identify and document conflicting functions, such as the ability to initiate, authorise, execute and verify transactions. Ensure that segregation of duties is enforced physically and logically where appropriate.
3. Ensure that procedures address the maintenance of appropriate segregation of duties and responsibilities during periods when regular personnel are unavailable (e.g., vacations, illness or leaves of absence).
4. Review the impact on segregation of duties and reassign responsibilities where necessary when job roles and responsibilities are created or updated as a result of changing business needs or reorganisation.
5. Design and implement compensating controls (e.g., regular review of individuals' activities by senior IT management) where the size or nature of the IT function precludes full 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

Control Practices

1. Ensure that the IT function is staffed and directed by experienced and qualified personnel, and all the necessary resources are co-ordinated.
2. Regularly review the staffing requirements (i.e., number of resources, skills) of the IT function, giving consideration to the business/IT environment and strategy.
3. Evaluate sourcing strategies, including outsourcing, co-sourcing or insourcing opportunities. In evaluating staffing requirements, ensure that management considers cost-effective internal sourcing activities, such as business/IT staff co-location, cross-functional training and job rotation.
4. Ensure that senior business and IT management reviews the results of the staffing evaluations and sourcing strategies, and implements appropriate actions within a reasonable time frame.

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

Control Practices

1. Identify key processes, the individual(s) supporting the processes and critical areas that lack job redundancy. Ensure that management periodically reviews key processes to identify which are critical to the organisation and considers the availability of individuals with the relevant skills, experience and knowledge to fulfill the critical roles.
2. Identify the availability of qualified resources with the appropriate skills, experience and knowledge, who could provide job redundancy for key processes.
3. Ensure that outsourcing or other arrangements have been made to provide job redundancy for key processes when required.
4. Ensure appropriate availability and coverage of staff to support key programmes, projects and processes, such as considering coverage during time-off requests, vacations and leaves of absence.
5. Ensure the periodic update of contact lists that include the primary personnel and alternative contacts (e.g., backup personnel, third parties) for key processes.
6. Ensure the creation and maintenance of documentation such as job procedures for key processes. Backup personnel are cross-trained on their job responsibilities to support other key processes when required.

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

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

Control Practices

1. Implement policies and procedures that describe when, how and what type of work can be performed or augmented by consultants and/or contractors, in accordance with the organisation's enterprisewide IT procurement policy.
2. Require contractors to comply with the organisation's policies and procedures (e.g., requirements for security clearance, physical and logical access control requirements, client equipment and personnel, information confidentiality requirements, and nondisclosure agreements). At the commencement of the contract, the contractor formally agrees to be bound by the organisation's IT policies. 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.
3. Provide contractors with a clear definition of their roles and responsibilities as part of their contracts. Contractors are explicitly required to document their work to agreed-upon standards and formats.
4. Ensure that an individual with appropriate authority within the IT function has responsibility for reviewing the contractor's work and approving payments.

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

Control Practices

1. Ensure that IT management has identified the key stakeholders (i.e., users, suppliers, security officers, risk managers, regulators) inside and outside the IT function.
2. Ensure that ownership and accountability for relationships between IT and key stakeholders are effectively managed. Appropriately skilled and experienced IT personnel are assigned to key stakeholders, giving consideration to the complexity and significance of the relationship to the IT function.
3. Establish and implement a plan to co-ordinate and communicate activities for the key stakeholders to assist them in supporting the organisation's strategic initiatives.
4. Establish an appropriate forum (i.e., conference calls, *ad hoc* meetings, focus groups) that facilitates IT-related activities and communications amongst various internal and external stakeholders.
5. Obtain regular feedback from key stakeholders to drive continuous improvement in the IT function and relationship management. For contractual (e.g., suppliers) and quasicontractual (e.g., internal service level agreements) relationships, hold regular formal meetings to assess performance and agree on improvement plans.

PO5 Manage the IT Investment

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

Control Practices

1. Define a framework, process and responsibilities to:
   - Drive IT budgeting and cost and benefit management
   - Enable fair, transparent, repeatable and comparable estimation of IT costs and benefits for input to the portfolio of IT-enabled business programmes (including a cost structure)
   - Maintain the IT asset and services portfolios and ensure that their maintenance is reflected in budgets and plans
2. Define inputs, outputs and processes inherent in the framework, and make regular updates based on available financial information.
3. Create and maintain portfolios of IT-enabled investment programmes, IT services and IT assets, which form the basis for the current IT budget and support the IT tactical and strategic plans.
4. Establish and use a process to use financial and portfolio information to provide input to business cases for new investments in IT assets and services throughout their full economic life cycle.
5. Work with service delivery managers to maintain the service portfolios and with operations managers and architects to maintain the asset portfolios, and provide an information prioritisation process of investment decisions.
6. Record and maintain the current IT budget, including committed expenditures and expenditures to date, considering:
   - IT projects recorded in the IT-enabled investment portfolios
   - Operation of and maintenance to asset and service portfolios
7. Use the financial framework and processes to provide fair, transparent, repeatable and comparable input on cost and benefits to business cases for new investments, in co-operation with the business.
8. Establish procedures to communicate the cost, benefit and risk-related aspects of these portfolios to the budget prioritisation, cost management and benefit management processes.

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

Control Practices

1. Create a process and establish a decision-making body for the prioritisation of IT initiatives and related resources within the high-level budget envelopes for IT-enabled investment programmes, IT services and IT assets as established by the strategic and tactical plans and maintained by portfolio decisions.
2. Create and use procedures to rank all IT initiatives within portfolios based on the business cases and strategic and tactical plans, and establish procedures to determine budget allocations and cut-off based on the envelopes received. Establish the procedure to communicate budget decisions and review them with the detailed IT budget holders.
3. Identify, communicate and resolve significant impacts of budget decisions on business cases, portfolios and strategy plans, e.g., when budgets are not aligned with strategic objectives or when budget allocations significantly impact the business case objectives.
4. Obtain ratification from the executive committee for the overall IT budget changes that negatively impact the entity's strategic or tactical plans and 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

Control Practices

1. Implement a methodology to establish, change and approve a formal IT budget, including all expected IT costs of IT-enabled investment programmes, IT services and IT assets as directed by the strategy, programmes and portfolios.
2. When creating the budget, consider the following components:
   - Authorised sources of funding
   - Internal resource costs, including people, information assets and accommodations
   - Third-party costs, including outsourcing contracts, consultants and service providers
   - Capital and operational expenses
   - Cost elements that depend on the workload
3. Document the rationale to justify contingencies and regularly review them.
4. Monitor the effectiveness of the different aspects of budgeting (project cost allocation, service cost allocation and budget variance analysis), and use the results to implement improvements to ensure that future budgets are more accurate, reliable and cost-effective.
5. Instruct process, service and programme owners as well as project and asset managers to plan budgets.
6. Review the budget plans, make decisions about budget allocations, and compile and communicate the overall IT budget.

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

Control Practices

1. Define a framework that defines which costs are included in IT, how they are allocated across budgets and projects, and how they are captured. The framework should also define how to analyse, report (to whom and how) and use the budget control and benefit management processes.
2. Ensure proper authority and independence between the individuals who capture, analyse and report financial information, and the IT budget holders.
3. Establish timescales for the operation of the cost management process in line with budgeting and accounting requirements. Within IT projects, the timescales for cost management are structured according to the deliverables timetable.
4. Define a method for the collection of relevant data to identify deviations for:
   - Budget control between actuals and budget
   - Benefit management of:
     - Actuals vs. targets for investments for solutions, possibly expressed in terms of ROI, not present value (NPV) or internal rate of return (IRR)
     - The actual trend of service cost for cost optimisation of services (e.g., defined as cost per user)
     - The actual trend of service portfolio cost for service delivery productivity improvements
     - Actuals vs. budget for responsiveness and predictability improvements of solutions delivery
   - Cost distribution between direct and indirect (absorbed and unabsorbed) costs
5. Define the systems from which the data are collected (financial accounting systems, time recording systems, IT asset registers, asset utilisation records, etc.).
6. Define how costs are consolidated for the appropriate levels in the organisation and how they will be presented to the stakeholders. The reports provide information to enable the timely identification of required corrective actions.
7. Instruct those responsible for cost management to capture, collect and consolidate the data, and present and report them to the appropriate budget, project or programme owners. Budget analysts and owners jointly analyse deviations and compare performance to internal and industry benchmarks. The result of the analysis provides an explanation of significant deviations and the suggested corrective actions.
8. Ensure that the appropriate level of management reviews the results of the analysis and approves suggested 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

Control Practices

1. Develop metrics for monitoring IT's contribution to the business case and establish in co-operation with all stakeholders:
   - Targets that reflect on the required IT capabilities and, where possible, are easy to translate into business capability targets
   - Trends in terms of cost reduction and the satisfaction of IT's customers with the services delivered
   - Post-implementation reviews for IT projects
2. Assign accountability for achieving benefits as recorded in the business case. Track and record in the business case how benefits change through the life cycle of programmes and projects and how they compare to internal and industry benchmarks.
3. Communicate the underlying reasons for measuring and monitoring selected benefits and the remediation process for identified deviations.
4. Implement corrective action when benefits significantly deviate:
   - For IT-enabled investment programmes—Update the business case of the project and the programme, and inform those responsible for portfolio management.
   - For IT service delivery—Initiate improvement.
5. Consider obtaining guidance from external experts, industry leaders and comparative benchmarking data to test and improve the metrics and targets.
6. Identify, quantify and qualify benefits of delivering IT solutions, providing IT services and managing IT assets as IT's contribution to the business case.

PO6 Communicate Management Aims and Direction

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

Control Practices

1. Align the IT management and control environment with the organisation's general risk and control environment.
2. Assign accountability and responsibility, including supervisory roles for creating procedures and practices to operationalise the control framework.
3. Ensure that the environment clearly defines the control culture and philosophy of the enterprise, risk appetite, ethical values, code of conduct, accountability, and requirements for management integrity in the IT management and control environment.
4. Create an approach for the communication of policies and procedures supported by appropriate awareness training to ensure transparency and understanding of these policies.
5. Ensure that the organisational structure for defining and developing the control framework clearly defines key areas of authority and responsibility.
6. Ensure that the human resources environment fosters and supports the adherence to policies and procedures.

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

Control Practices

1. Define an IT risk and control framework adopting relevant guidance such as the Committee of the Sponsoring Organisations of the Treadway Commission's (COSO's) *Internal Control—Integrated Framework*, COSO's *Enterprise Risk Management—Integrated Framework* and COBIT.
2. Ensure that the enterprise IT risk and control framework specifies:
   - Purpose of the internal control framework
   - Scope of the control framework (i.e., IT process framework)
   - Management's expectation of what needs to be controlled
   - Roles and responsibilities
   - Methodologies to be used
3. Ensure the aim at maximising success of value delivery while minimising risks to information assets through preventive measures, timely identification of irregularities, limitation of losses and timely recovery of business assets.

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

Control Practices

1. Create a hierarchical set of policies, standards and procedures to manage the IT control environment. The form and style of the policies should align to the IT control environment.
2. Develop specific policies on relevant key topics such as quality, security, confidentiality, internal controls, ethics and intellectual property rights.
3. Evaluate and update the policies at least yearly to accommodate changing operating or business environments. The re-evaluation should assess the policies' adequacy and appropriateness, and they should be amended as necessary.
4. Ensure that procedures are in place to track compliance with policies and define the consequences of non-compliance.
5. Ensure that accountability has been defined through roles and responsibilities.

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

Control Practices

1. Ensure that policies are effectively translated into operational standards.
2. Ensure that employment contracts are aligned with policies.
3. Capture explicit acknowledgement from users as to their receipt and understanding of the policies, procedures and standards.
4. Ensure that sufficient and skilled resources are available to support the rollout process. Rollout methods should address resource and awareness needs and implications.

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

Control Practices

1. Establish a programme to continuously communicate IT objectives and direction that is supported by top management in action and words, using all available channels.
2. Ensure that the information communicated encompasses a clearly articulated mission, service objectives, security, internal controls, quality, code of ethics/conduct, policies and procedures, etc. Communicate the information at the appropriate level of detail for the respective audiences within the enterprise.
3. Ensure that sufficient and skilled resources are available to support the communication process.

PO7 Manage IT Human Resources

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

Control Practices

1. Develop and maintain an IT human resources management plan that includes a definition of the skill requirements and preferred professional qualifications to meet the tactical and strategic IT needs of the organisation. Regularly review the currently available skills against the requirement for skilled resources.
2. Implement a formal and documented process for the recruitment and retention of IT personnel that meets regulatory requirements and is compatible with the organisation's human resources policies.
3. Develop and maintain IT human resource retention practices focusing on critical and scarce skills, considering personal evaluations, compensation and incentives, personal development plans, and individual training needs.

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

Control Practices

1. Define and maintain the skills, competencies and qualifications required for each role within the IT organisation as part of job descriptions.
2. Periodically review the skills, competencies and qualifications of current personnel, and compare to requirements.
3. Provide appropriate education and training to maintain adequate competence and, where appropriate, encourage skills certification.
4. Provide formal career planning to encourage competency development, opportunities for personal advancement and reduced dependence on key individuals.

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

Control Practices

1. Define and regularly maintain descriptions of IT roles covering responsibilities to highlight any specific risk management, security and compliance requirements.
2. Ensure that IT personnel acknowledge and document, upon hiring and periodically thereafter, their acceptance of role descriptions and responsibilities.
3. Ensure that terms and conditions of employment stress the employee's responsibility for information security, internal control and regulatory compliance, and address the assignment of all intellectual property rights to the organisation and non-disclosure of confidential information.
4. Ensure that supervision for each role within IT is based on the risks posed by that role and is effected by an appropriate mechanism, including personal supervision, review of work, dual performance of tasks and/or automated monitoring.

PO7 Manage IT Human Resources (cont.)

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

Control Practices

1. Determine training and awareness requirements most critical to accomplishing the organisation's goals, and put a process in place to measure against expected levels the completion of training and the level of awareness within different user groups. The process may include certification and recertification at appropriate intervals, as well as the need for continued education to maintain certification.
2. Develop and deliver a programme to maintain personnel knowledge about the organisation's requirements for internal control and ethical conduct.
3. Develop and deliver a security requirements programme to educate all IT employees prior to granting access to IT resources and facilities. The programme should educate all new employees on:
   - The impact on the organisation and the employee if the security requirements are not met
   - Appropriate use of IT resources and facilities
   - How security incidents should be handled and escalated
   - Ethical use of IT resources and facilities
   - The employee's responsibilities for information security
4. Review training materials and programmes regularly for adequacy with respect to changing business requirements and their impact on necessary knowledge, skills and abilities.

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

Control Practices

1. Identify key roles and personnel within the IT organisation related to critical IT processes or identified as single points of reliance within the IT organisation.
2. Provide relevant and appropriate training to reduce dependence on key resources (e.g., cross-training and training of backups).
3. Enforce documentation of key tasks for critical roles.
4. Encourage job rotation, succession planning and sharing of knowledge for critical roles.
5. Ensure that key staff members in critical roles take reasonable holiday leave and that their positions are backed up with a suitable replacement.

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

Control Practices

1. Define the criteria for determining the roles that require clearance procedures.
2. Undertake the clearance procedure for all staff members who perform a role that requires clearance. Maintain documentation in personnel records.
3. For sensitive roles, if appropriate, periodically repeat the clearance procedure.

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

Control Practices

1. Set individual goals based on SMARRT objectives that reflect core competencies, company values and skills required for the role(s).
2. Provide specific instructions for the use and storage of personal information in the evaluation process, in compliance with applicable personal data and employment legislation.
3. Compile performance evaluation results from across the IT organisation for use in the review of current competencies and training requirements.
4. Provide appropriate feedback regarding performance against the individual's goals.
5. Implement a remuneration/recognition process that rewards successful attainment of performance goals and is applied consistently and in line with organisational policies.
6. Develop performance improvement plans based on the results of the evaluation process and identified training and skills development requirements.

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

Control Practices

1. Include the need for job change and termination procedures within human resource policies.
2. Document and implement exit procedures for termination of employment that include reassignment of job duties so disruptions are minimised and job transfer procedures including necessary knowledge transfer, timely securing of logical and physical access, security of the organisation's assets, and exit interviews.
3. Design job change procedures to ensure efficient continuation with minimal disruption, providing guidance on the need for job mentoring, job handover steps and preparatory formal training.
4. Include in job change procedures confirmation that logical and physical access privileges have been revised and aligned with the new job requirements.

PO8 Manage Quality

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

Control Practices

1. Develop and document a QMS, with input from IT management and external and internal stakeholders, that is consistent with relevant enterprisewide quality frameworks, to encourage a standardised and continuous approach to quality.
2. Endorse the QMS and effectively communicate the approach (e.g., through regular, formal quality training programmes).
3. For each important process, project or objective, define an appropriate quality plan that is in alignment with the enterprise quality management criteria and policies.
4. Regularly review the continued relevance, efficiency and effectiveness of specific quality management processes. Monitor the achievement of quality objectives.
5. Identify and document root causes for non-conformance, and communicate findings to IT management and other stakeholders in a timely manner to enable remedial action to be taken. Where appropriate, perform follow-up reviews.
6. Benchmark the results of the quality reviews against industry guidelines, standards and similar types of enterprises.

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

Control Practices

1. Define and implement appropriate IT standards that are aligned with the QMS.
2. Define the requirements and circumstances for adherence to, or non-compliance with, adopted IT standards, and require authorisation and monitoring of deviations.
3. Ensure that changes and/or updates to adopted IT standards are reflected in and consistent with the intent of the QMS.
4. Ensure that QMS standards, policies, processes and practices are continuously applied to all phases of projects and all services.

PO8 Manage Quality (cont.)

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

Control Practices

1. Apply development and acquisition standards for changes to existing IT resources. Ensure that there is flexibility within the standard system development life cycle (SDLC) to cope with projects of various sizes and types.
2. Create policies and procedures as part of the development and acquisition standards that provide appropriate and 'fit for purpose' guidelines for controlled development and acquisition of IT solutions.
3. Incorporate guidance into IT standards for the acquisition of the technology infrastructure components that provide alignment with business requirements, quality practices, industry knowledge, guidelines and future technology direction.

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

Control Practices

1. Identify the customers for each IT operational service and new solution, and determine their quality acceptance criteria. Capture quality acceptance criteria for inclusion in SLAs.
2. Periodically obtain customer views on the IT standards and practices to ensure that they meet customer expectations.
3. Regularly monitor and review the QMS against agreed-upon acceptance criteria. Include feedback from customers, users and management. Respond to discrepancies in review results to continuously improve the QMS.
4. Include customer care skills, responsibilities and dispute resolution in staff 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

Control Practices

1. Develop an overall quality plan that encourages continuous improvement by learning from mistakes and sharing best practices.
2. Identify recurring examples of quality defects, determine their root cause, and agree on improvement actions with the service and project delivery teams.
3. Identify examples of excellent quality delivery processes that can benefit other services or projects, and share these with the service and project delivery teams to encourage improvements.

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

Control Practices

1. Define and maintain quantifiable, goal-driven quality metrics (or measurements) aligned to overall quality objectives covering the quality of individual projects and services.
2. Ensure that management and process owners regularly review QMS performance against defined quality metrics.
3. Analyse overall quality performance results to determine:
   - The extent of compliance with the QMS
   - Trends indicating quality strengths and weaknesses
   - The effectiveness of the QMS in identifying quality problems
   - Efficiency in timely identification of faults
   - Management commitment to ongoing QMS performance and improvement

PO9 Assess and Manage IT Risks

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

Control Practices

1. Make sure the IT risk management framework fits with the risk management objectives of the enterprise. Use similar risk classification principles and, wherever possible, classify and manage IT risks in a business-driven hierarchy, for example:
   - Strategic
   - Programme
   - Project
   - Operational
2. Define standard scales for IT risk assessment, covering impact and probability aligned with the enterprise risk management framework.
3. Align the IT risk management appetite and tolerance levels with the enterprise risk management framework.

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

Control Practices

1. Evaluate risks qualitatively according to their impact (catastrophic, critical, marginal), probability (very likely, probable, improbable) and time frame (imminent, near term, far term), or quantitatively, when appropriate probability data exist.
2. Prioritise risks by separating the 'vital few' from the rest and ranking them based upon a criterion or criteria established by the project team. Techniques for prioritisation include comparison risk ranking, multivoting, and paring to the top 'n' and top five.
3. Perform risk assessment activities considering the context of the IT management processes that are affected.

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

Control Practices

1. Obtain agreement and sign-off from stakeholders of key events and their impacts.
2. Identify potential events that could negatively affect enterprise goals or operations considering results of former audits, inspections and identified incidents, using checklists, workshops, process flow analysis, or other tools and techniques.
3. Identify potential negative impacts that are relevant and significant for the enterprise for each of the selected events. Record and maintain the information in the risk registry, using the enterprise risk management framework terminology.
4. Involve appropriate cross-functional teams in the event and impact identification activity. Depending on the scope of the assessment, these teams may be composed of representatives from the IT, risk management and business functions.
5. Review all potential events as a whole to ensure completeness and to identify interdependencies that could affect impact and probability.

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

Control Practices

1. Determine the likelihood of identified risks qualitatively (e.g., very likely, probable, improbable) or quantitatively using statistical analysis and probability determinations, based on reasonable sources of information that can be appropriately validated.
2. Determine the material impact on the business of identified risks qualitatively (e.g., catastrophic, critical, marginal) or quantitatively (e.g., impact on revenue or shareholder value).
3. Assess risks inherent in the event and after considering the controls that are in place to identify the residual risks for which a risk response will need to be determined.
4. Document the results of the risk assessment, showing the method followed to come to the conclusions.

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

Control Practices

1. Consider the results of the risk assessment and determine a strategy for mitigating the risks, considering the significance of the risk and the probable cost and benefit of one of more of the options—avoidance, reduction, sharing and acceptance—that aligns with strategic objectives and is in keeping with the enterprise's accepted risk management culture and risk tolerances.
2. Develop a risk action plan to implement the agreed-upon risk response based on a consideration of:
   - Priorities
   - Existing controls that could be improved or modified
   - Practical implementation considerations
   - Any specific legal, regulatory or contractual requirements
   - Probable costs
   - Potential benefits

PO9 Assess and Manage IT Risks (cont.)

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

Control Practices

1. Develop the risk action plan containing prioritised risk responses. Identify priorities, responsibilities, schedules, expected outcome of risk mitigation, costs, benefits, performance measures and the review process to be established.
2. Obtain approval for recommended risk response actions from appropriate authorities. Define and document ownership for approved plan activities, and inform affected parties.
3. Ensure that accepted risks are formally recognised, approved by senior management and recorded.
4. Monitor execution of the action plan, report progress and deviations to senior management, and adjust the plan accordingly.
5. Periodically review the action plan:
   - To ensure that it continues to efficiently and effectively address the IT risks identified
   - In light of any changes to business objectives or relevant IT systems
   - To identify improvement opportunities to the risk assessment and management process

PO10 Manage Projects

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

Control Practices

1. Define and document the programme, including all the projects required to achieve the programme's expected business outcomes. Specify required resources, including funding, project managers, project teams, IT resources and business resources where applicable. Gain formal approval of the document from key business and IT stakeholders.
2. Assign accountability clearly and unambiguously for each project, including achieving the benefits, controlling the costs, managing the risks and co-ordinating the project activities.
3. Determine the interdependencies of multiple projects in the programme, and develop a schedule for their completion that will enable the overall programme schedule to be met.
4. Determine programme stakeholders inside and outside the enterprise, and establish and maintain appropriate levels of co-ordination, communication and liaison with these parties.
5. Verify periodically with the business that the current programme as designed will meet business requirements and make adjustments as necessary. Review progress of individual projects and adjust the availability of resources as necessary to meet scheduled milestones.

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

Control Practices

1. Ensure that the project management framework is consistent with, and is an integral component of, the organisation's programme management framework.
2. Ensure that the project management framework includes:
   - Guidance on the role and use of the programme or project office
   - A change control process for recording, evaluating, communicating and authorising changes to the project scope, project requirements or system design
   - Requirements for integrating the project within the overall programme
3. Ensure that the project management method covers, at minimum, the initiating, planning, executing, controlling and closing project stages, as well as checkpoints and approvals.

Control Objective	Value Drivers	Risk Drivers
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.	• 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	• 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

Control Practices

1. Prior to each project's initiation, establish a project management governance structure appropriate to the project's size, complexity and risks, including legal, regulatory and reputational risks.
2. Assign each IT project one or more sponsors with sufficient authority to manage execution of the project within the overall programme.
3. Define the responsibility and accountability of the programme sponsor, the project manager, and, as necessary, the steering committee and project management office.
4. To track the execution of a project, put in place mechanisms such as regular reporting and stage reviews that are the responsibility of the project manager to complete 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

Control Practices

1. Obtain the commitment and participation of key stakeholders, including management of the affected user department and key end users in the initiation, definition and authorisation of a project.
2. Outline during project initiation ongoing key stakeholder commitment and roles and responsibilities for the duration of the project life cycle. Ongoing involvement includes, but is not limited to, project approval, project phase approval, project checkpoint reporting, project board representation, project planning, product testing, user training, user procedures documentation and project communication material development.

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

Control Practices

1. Provide to the stakeholders a clear, written statement defining the nature, scope and business benefit of every project to create a common understanding of project scope amongst stakeholders.
2. Ensure that key stakeholders and programme and project sponsors within the organisation and IT agree upon and accept the requirements for the project, including definition of project success (acceptance) criteria and key performance indicators.
3. Ensure that the project definition describes the requirements for a project communication plan that identifies internal and external project communications.
4. With the approval of stakeholders, maintain the project definition throughout the project, reflecting changing requirements.

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

Control Practices

1. Gain approval and sign-off on the deliverables produced in each project phase from designated managers and customers of the affected business and IT functions.
2. Base the approval process on clearly defined acceptance criteria agreed to by key stakeholders prior to work commencing on the project phase deliverable.
3. Assess whether the project is on schedule, within budget and aligned with the agreed-upon scope. Assess identified variances and identify the impact on the project plan and realisation of expected benefits.
4. Assess the project at agreed-upon major review points, and make formal 'stop/go' decisions based on predetermined critical success criteria.

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

Control Practices

1. Develop a project plan that provides information to enable management to control project progress. The plan should include details of project 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. Identify interdependencies of resources (e.g., key personnel) and deliverables with other projects.
2. Maintain the project plan and any dependent plans to ensure that they are up to date and reflect actual progress and material changes.
3. Ensure that there is effective communication of project plans and progress reports amongst all projects and with the overall programme. Ensure that any changes made to individual plans are reflected in the other plans.

PO10 Manage Projects (cont.)

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

Control Practices

1. Identify resource needs for the project and clearly map out appropriate roles and responsibilities, with escalation and decision-making authorities agreed upon and understood.
2. Identify required skills and time requirements for all individuals involved in the project phases in relation to defined roles. Staff the roles based on available skills information (e.g., IT skills matrix).
3. Utilise experienced project management and team leader resources with skills appropriate to the size, complexity and risk of the project.
4. Consider and clearly define the roles and the responsibilities of other involved parties, including finance, legal, procurement, human resources, internal audit and compliance.
5. Clearly define and agree upon the responsibility for procurement and management of third-party products and services, and manage the relationships.

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

Control Practices

1. Establish a formal project risk management framework that includes identifying, analysing, responding to, mitigating, monitoring and controlling risks.
2. Assign to appropriately skilled personnel the responsibility for executing the organisation's project risk management framework within a project. Consider allocating this role to an independent team, especially if an objective viewpoint is required or a project is considered critical.
3. Perform the project risk assessment of identifying and quantifying risks continuously throughout the project. Manage and communicate risks appropriately within the project governance structure.
4. Reassess project risks periodically, including at entry into each major project phase and as part of major change request assessments.
5. Identify risk and issue owners for responses to avoid, accept or mitigate risks.
6. Maintain and review a project risk register of all potential project risks, and maintain a log of all project issues and their resolution. Analyse the log periodically for trends and recurring problems, to ensure that root causes are corrected.

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

Control Practices

1. Identify ownership and responsibilities, quality review processes, success criteria and performance metrics, to provide quality assurance for the project deliverables.
2. Define any requirements for independent validation and verification of the quality of deliverables in the plan.

PO10 Manage Projects (cont.)

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

Control Practices

1. Establish a standard change request form and request process requiring documentation of the requested change and the expected benefits of the change. The programme management team should designate the individuals (business stakeholders, IT personnel) authorised to make project change requests.
2. Review change requests and estimate the potential effects on the project, including resource requirements and impact on schedule. Document the estimated project impact in the change request.
3. Review the completed change request and document the approval or denial of the request by key stakeholders, including business project sponsor and IT project manager.
4. Consider and approve at the programme level all approved project change requests based on an assessment of the effect the change will have on the other projects. If the requested change should not be implemented, share the reasons with the requesting project management team so they can evaluate alternative approaches.
5. Update the project and programme plans for all approved changes, and communicate approved changes to all business and IT stakeholders in a timely manner.

Control Objective	Value Drivers	Risk Drivers
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.	• 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	• Untrustworthy assurance activities • Ineffective and/or inefficient assurance activities • Accreditation and implementation delays

Control Practices

1. Define the assurance tasks required to ensure compliance with internal controls and security requirements that impact the systems or processes in the scope of the project. Include key compliance stakeholders in the definition and approval of assurance tasks.
2. Determine and document how the assurance tasks will be performed. Include appropriate subject matter specialists (e.g., audit, security or compliance) in the process.

PO10 Manage Projects (cont.)

Control Objective	Value Drivers	Risk Drivers
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.	• 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	• Ineffective reporting on project progress and unidentified issues • Lack of control over project progress • Loss of focus on customer expectations and business needs

Control Practices

1. Establish and use a set of project criteria as part of the programme management framework, including, but not limited to, scope, schedule, quality, cost and level of risk.
2. Measure project performance against key project performance criteria. Analyse deviations from established key project performance criteria for cause, and assess positive and negative effects on the programme and its component projects. Report to identified key stakeholders progress for the programme and component projects, deviations from established key project performance criteria, and positive and negative effects on the programme and its component projects.
3. Monitor changes to the programme and review existing key project performance criteria to determine if they still represent valid measures of progress. Document and submit any necessary changes to the programme's key stakeholders for their approval before adoption. Communicate revised criteria to project managers for use in future performance reports.
4. Recommend, implement and monitor remedial action, when required, in line with the programme and project governance framework.

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

Control Practices

1. Define and apply key steps for project closure, including post-implementation reviews that assess whether a project attained desired results and benefits.
2. Plan and execute post-implementation reviews to determine if projects delivered expected benefits and to improve the project management and system development process methodology.
3. Identify, assign, communicate and track any uncompleted activities required to achieve planned programme project results and benefits.
4. Collect from the project participants and reviewers the lessons learned and key activities that led to delivered benefits. Analyse the data and make recommendations for improving the project management method for future projects.

AI — Acquire and Implement

CONTROL PRACTICES

AI1 Identify Automated Solutions

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

Control Practices

1. Define and implement a requirements definition and maintenance procedure and a requirements repository that are appropriate for the size, complexity, objectives and risks of the business initiative that the organisation is considering undertaking. This procedure should take into account the nature of the enterprise's business, strategic direction, strategic and tactical IT plans, in-house and outsourced business and IT processes, emerging regulatory requirements, people skills and competencies, structure, business case, and enabling technology.
2. Confirm that all stakeholder requirements, including relevant acceptance criteria, are considered, captured, prioritised and recorded in a way that is understandable to the stakeholders, business sponsors and technical implementation personnel.
3. Confirm that the functional and technical requirements are considered, captured and prioritised.
4. Confirm that the requirements include aspects regarding:
   - Continuity
   - Legal and regulatory compliance
   - Performance
   - Reliability
   - Compatibility
   - Auditability
   - Security and risk management
   - Availability
   - Ergonomics
   - Operability and usability
   - Safety
   - Documentation (end user, operations, deployment, configuration)

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

Control Practices

1. Use a holistic approach to risk analysis, ensuring that business, technology and project risks are properly identified, examined, assessed and understood by all stakeholders.
2. Consider as part of the risk analysis the impact of the project (development or acquisition, implementation, operation, retirement, and disposal) on the organisation's risk profile and threats to data integrity, security, availability, privacy, and compliance with laws and regulations.
3. Consider appropriate business, functional, technical and project risk mitigation activities as part of the definition of the possible solutions.

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

Control Practices

1. Define and execute a feasibility study that clearly and concisely describes the key alternative courses of action that will satisfy the business and functional requirements with an evaluation of their technological and economic feasibility. Identify required actions for the acquisition or development, and take into account scope and/or time and/or budget limitations.
2. Review the alternative courses of action with all stakeholders, and select the most appropriate one based on feasibility criteria, including risks and cost.
3. Translate the preferred course of action into a high-level acquisition/development plan identifying resources to be used and stages requiring a go or no-go decision.

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

Control Practices

1. Obtain sign-off from the business sponsor and technical authority for the proposed approach, and gather feedback requiring further feasibility analysis.
2. Perform quality reviews at the end of each key project stage to assess the results against the original acceptance criteria. Business sponsors and other stakeholders should sign off on each successful quality review.

AI2 Acquire and Maintain Application Software

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

Control Practices

1. Establish a high-level design specification that translates the business requirements for the software development based on the organisation's technological direction and information architecture model.
2. Confirm that the design approach and documentation are compliant with the organisation's design standards.
3. Involve appropriately qualified and experienced users in the design process to draw on their expertise and knowledge of existing systems or processes.
4. Confirm that the design is consistent with the business plans, strategies, applicable regulations and IT plans.
5. Ensure that the high-level design is approved and signed off on by IT stakeholders (e.g., human/computer interaction, security and other experts) to ensure that their inputs have been recognised and the design, as a whole, constitutes a solution that the organisation can deliver, operate and maintain. Establish that no project proceeds to the business approval process without appropriate review and sign-off by IT stakeholders.
6. Submit the final high-level design after QA sign-off to the project sponsor/business process owner, and obtain approval and sign-off. Establish that no project proceeds to development without appropriate sign-off by the business.

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

Control Practices

1. Classify data inputs and outputs according to information architecture and data dictionary standards.
2. Assess the impact on existing applications and infrastructure during the process of gathering requirements and designing the solution, and design appropriate integration approaches. Address integration of the planned application system with existing or planned co-operating applications and infrastructure, including packaged software acquired from third parties. Consider the impact of differing update cycles.
3. Specify the source data collection design, documenting the data that must be collected and validated for processing transactions as well as the methods for validation. Consider data inputs from existing programs, packaged software, external parties, web forms, etc.
4. Define system availability requirements, and design appropriate redundancy, failure recovery and backup processing arrangements.
5. Define file and database requirements for storage, location and retrieval of data. Consider availability, control and auditability, security, and network requirements.
6. Define the processing steps, including specification of transaction types and processing rules incorporating logic transformations or specific calculations. Consider availability, control and auditability, logging, and audit trails.
7. Based on the user requirements and taking into account the different types of recipients, usage, details required, frequency, method of generation and other design details, define the data requirements for all identified outputs. Appropriate design requirements should guarantee the availability, completeness, integrity and confidentiality of output data. Consider the impact of data outputs to other programs, external parties, etc.
8. Design the interface between the user and the system application so that it is easy to use and self-documenting. Consider the impact of system-to-system interface design on infrastructure performance, including the capacity of personal computing devices and network bandwidth and availability.
9. Reassess system design whenever significant technological and/or logical discrepancies occur during design, development and maintenance. Results of the reassessment should be subject to the normal approval cycle.
10. Prepare and document detailed design specifications in accordance with organisational and industry-accepted specification standards and the information architecture.
11. Conduct a design walk-through with IT and business stakeholders before development is initiated, as a part of the sign-off process for the design specifications. Various aids can be used to assist with the sign-off, including prototypes, to aid stakeholder understanding of the final design.

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

Control Practices

1. Define all automated application controls (authorisation, input, processing and output) based on business process control requirements provided in the requirements documentation.
2. Define how business processes will need to be adjusted to use the automated control functions provided in purchased/packaged application software.
3. Confirm the design specifications for all automated application controls with IT technical authorities and business process owners, and obtain their approval and sign-off.
4. Confirm that the design includes automated controls within the application that support general control objectives (such as security, data integrity and audit trails), including access control mechanisms and database integrity controls. Confirm that the design has received sign-off from relevant technical design authorities and approval of the business process owner.
5. Assess design specifications of automated application and general controls against internal audit, control, and risk management standards and objectives. Consider the effect of compensating controls outside the application software realm.

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

Control Practices

1. Design approaches and solutions to security and availability that adequately meet the defined requirements. These approaches should take into account the organisational security architecture and policies, industry security and privacy best practices, and regulatory and compliance requirements for security and privacy.
2. Consider the security and availability infrastructure already in place. Where possible, build on and extend these capabilities.
3. Consider access rights and privilege management, protection of sensitive information at all stages, authentication and transaction integrity, and automatic recovery.
4. Define how the solutions for security and availability in the infrastructure will be integrated with the application, paying particular attention to transactions, local and wide area networks (e.g., Internet), shared and federated databases, access control mechanisms, load detection, and recovery mechanisms.
5. Confirm the design of security, availability, access management, authentication and protection of transaction integrity with IT technical authorities and, as appropriate, subject matter experts. Obtain their sign-off on and approval of the design. Also confirm with business process owners that the design meets their security and availability requirements using non-technical walk-throughs, where necessary, to confirm understanding.

AI2 Acquire and Maintain Application Software (cont.)

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

Control Practices

1. Assess the impact of any major upgrade and classify it according to agreed-upon objective criteria (such as business requirements), based on the outcome of analysis of the risk involved (such as impact on existing systems and processes or security), cost-benefit justification and other requirements. Follow normal system development and implementation processes as appropriate for the nature of the change.
2. Consider interoperability with existing applications and databases, appropriate user interfaces, and efficient utilisation of technology resources (e.g., security framework and standards, availability, access management, auditability, networks and storage) in the design specification.
3. Consider the impact of customisation and configuration on the performance and efficiency of the acquired packaged application software and on existing applications. operating systems and other infrastructure.
4. Consider the effect of contractual terms with the vendor on the design of customisation and configuration.
5. Consider the availability of source code for purchased/packaged applications in the customisation and configuration process. Review contractual arrangements with the vendor. Consider escrow arrangements where the source code is not available. Assess the risks in the event that the acquired application packaged software is no longer available at the expiry of a contract or for other reasons.
6. Ensure that testing procedures cover verification of acquired application control objectives (such as functionality, interoperability with existing applications and infrastructure, system performance efficiency, integrated capacity and load stress testing, and data integrity).
7. Conduct a design walk-through with IT and business stakeholders before customisation is initiated, as a part of the sign-off process for the customisation and configuration of application software specifications.
8. Consider whether the implications of customisation and configuration require reassessment of strategies for acquired application packaged software.
9. Obtain approval of business process owners for detailed design specifications for customisation and configuration of application software.
10. Ensure that user and operational manuals (online help) are complete and updated where necessary to account for any customisation or special conditions unique to the implementation.
11. Consider when the effect of cumulative customisations and configurations (including minor changes that were not subjected to formal design specifications) require a high-level reassessment of the acquired solution and associated functionality. Assess whether these changes trigger the development of a detailed design specification for customisation and configuration of the application software. Assess whether these changes restrict the ability of the organisation to adopt vendor upgrades to purchased applications packaged software.

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

Control Practices

1. Assess the impact of any major upgrade and classify it according to specified objective criteria (such as business requirements), based on the outcome of analysis of the risk involved (such as impact on existing systems and processes or security), cost-benefit justification and other requirements. Follow normal system development and implementation processes as appropriate for the nature of the change.
2. Obtain agreement on and approval of the implementation of the development and implementation process with the business process sponsor and other affected stakeholders. Ensure that the business process owners understand the effect of designating changes as maintenance or major upgrades.

AI2 Acquire and Maintain Application Software (cont.)

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

Control Practices

1. Establish development procedures to ensure that the development of application software adheres to organisational development standards.
2. Ensure that application software is developed based on agreed-upon specifications and business, functional and technical requirements.
3. Establish agreed-upon stages of the development process (development checkpoints). At the end of each stage, facilitate formal discussions of approved criteria with the stakeholders. Obtain approval and sign-off from all stakeholders following successful completion of functionality, performance and quality reviews before finalising stage activities. At the final stage, confirm with IT technical authorities and operations management that the applications are ready and suitable for migration to the production environment.
4. Assess the adequacy of software developed in terms of its compatibility and ease of integration with existing applications and infrastructure.
5. When third-party developers are involved with the applications development, establish that they adhere to contractual obligations and organisational development standards and that licensing requirements have been addressed.
6. Monitor all development activities and track change requests and design, performance and quality reviews, ensuring active participation of all impacted stakeholders, including business process users and IT technology representatives.
7. Ensure that requested changes arising within IT or from the business process owner are tracked.
8. Consider the effect of dynamic, non-sequential development techniques (e.g., rapid application development, extreme programming) on the monitoring of the application development progress and approval of application software by stakeholders.

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

Control Practices

1. Define a software QA plan. Ensure that the plan includes:
   - Specification of quality criteria
   - Validation and verification processes
   - Definition of how quality will be reviewed
   - Necessary qualifications of quality reviewers
   - Roles and responsibilities for the achievement of quality

   Consider:
   - The effect of embedding quality within the development process
   - The presence or absence of formal review by independent QA teams
   - Ensuring that reviewers are independent from the development team
2. Design a process that monitors the software quality based on:
   - Project requirements
   - Enterprise policies
   - Adherence to site development systems methodologies
   - Quality management procedures and acceptance criteria
3. Employ code inspection, programme walk-throughs and testing of applications. Report on outcomes of the monitoring process and testing to the application software development team and IT management.
4. Monitor all quality exceptions. Ensure that corrective actions are taken. Maintain a record of all reviews, results, exceptions and corrections. Repeat quality reviews, where appropriate, based on the amount of rework and corrective action.

AI2 Acquire and Maintain Application Software (cont.)

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

Control Practices

1. Design a process for standardising, tracking, recording and approving all change requests during development of application systems.
2. Assess the impact of all project change requests, and categorise and prioritise them accordingly.
3. Track changes to requirements for development projects, enabling all stakeholders to monitor, review and approve the changes. Ensure that the outcomes of the change process are fully understood and agreed to by the stakeholders.

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

Control Practices

1. Design an effective and efficient process for application software maintenance activities. Prioritise maintenance activities, paying attention to business needs and resource requirements. Ensure that all changes in software comply with the formal change management process, including impact on other systems and infrastructure. Ensure that risk and security requirements and interdependencies are addressed.
2. Monitor all maintenance changes. If appropriate, aggregate maintenance tasks into a single ‘change’ to make management and control easier. Ensure that any major maintenance is categorised and managed as a formal redevelopment.
3. Establish the review and approval of all emergency or any other changes applied without adherence to the formal change process.
4. Ensure that the pattern and volume of maintenance activities are analysed periodically for abnormal trends indicating underlying quality or performance problems.
5. Establish processes to ensure that all maintenance activity is completed successfully and thoroughly. Track maintenance activities to ensure completion. Where necessary, update user systems and operational documentation.

AI3 Acquire and Maintain Technology Infrastructure

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

Control Practices

1. Create and maintain a plan for the acquisition, implementation and upgrade of technology infrastructure that meets established business functional and technical requirements and is in accord with the organisation's technology direction. The plan should also consider future flexibility for capacity additions, transition costs, technical risks and, for technology upgrade purposes, the lifetime of the investment. The plan should be integrated with the organisation's strategic and operational planning processes.
2. Ensure that the plan includes a financial appraisal stating the ROI over the expected lifetime of the infrastructure.
3. Review all acquisition plans considering risks, costs, benefits and technical conformance with corporate technology standards. Any deviations should be authorised by the IT architecture board. Approve all reviewed and accepted plans with a formal sign-off.
4. Establish a feedback process to support continuous improvement and raise any suggested changes to the technology infrastructure plan, technology guidelines and standards.

AI3 Acquire and Maintain Technology Infrastructure (cont.)

Control Objective	Value Drivers	Risk Drivers
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.	• Consistent technological planning • Enhanced system security • Balanced hardware and software utilisation • Data integrity and confidentiality maintained in all system stages	• Disruptions in production processing • Undetected bypassing of access controls • Unauthorised access to sensitive software • Business needs not supported by technology

Control Practices

1. Back up and secure all infrastructure data and software prior to installation or maintenance tasks.
2. Test whether the application software environment is separated from, but sufficiently similar to, production to verify functionality and establish its security, availability or integrity conditions. This ensures that they operate appropriately and are in compliance with requirements established within the acquisition and maintenance framework for technology infrastructure. Analyse and follow vendor recommendations.
3. Assess all the security aspects associated with system software installation and maintenance processes, especially the modification of original passwords assigned by service providers and the setup of parameters that may affect security, such as vendor-established default parameter settings.
4. Monitor when temporary access is granted to allow installation, and ensure that passwords are changed as installation is completed.
5. Monitor that only appropriately licenced software is tested and installed. Review the process to ensure that system software installation is performed in accordance with vendor guidelines and any deviations are discussed with the vendor to assess potential impact.
6. Control movement of programs and data amongst libraries by ensuring that this is performed by an independent group (e.g., librarian).
7. Enforce acceptance procedures using objective acceptance criteria to ensure that product performance (including security and functionality) is consistent with the agreed-upon specifications and/or SLA requirements.
8. Provide appropriate training to personnel who use sensitive infrastructure components.
9. Monitor and log access and maintenance of sensitive infrastructure components, and ensure that these are regularly reviewed.

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

Control Practices

1. Establish a strategy and plan for infrastructure maintenance to provide overall guidance in line with the organisation's change management procedures.
2. Ensure that maintenance of the installed system software (patches, service packs and other updates) is managed through the established change management process and is performed in accordance with vendor procedures and guidelines by qualified and authorised internal and/or vendor personnel.
3. Maintain documentation of system software, and ensure that it is complete and current. Require vendors to deliver new and updated documentation each time the system software is maintained.
4. Maintain currency of system software by applying vendor upgrades or patches in a timely manner.
5. Review on a regular basis the amount of maintenance being performed and the vulnerability to unsupported infrastructure; consider future risks, including security vulnerabilities. Report any issues identified 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

Control Practices

1. Design an approach commensurate with the strategic technology plans that will enable the creation of suitable testing and simulation environments to help verify the feasibility of planned acquisitions or developments. Consider in-house and/or external options, including reference visits, vendor test labs, creation of prototypes, modelling, pilots and proof-of-concept developments, depending on the complexity, practicalities and costs.
2. Create a test environment that considers functionality, hardware and software configuration, integration and performance testing, migration between environments, version control, test data and tools, and security.

AI4 Enable Operation and Use

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

Control Practices

1. Define and document the operational procedures in advance of implementation, and establish them during acceptance tests to ensure that they are complete, accurate and usable.
2. Define and document the user procedures in advance of implementation, and establish them during acceptance tests to ensure that they are complete, accurate and usable.

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

Control Practices

1. Establish ownership of the system. Define management and administrative functions, security and control procedures, and training requirements.
2. Create management documentation, including roles and responsibilities, segregation of duties, business continuity considerations, access and privilege controls, administration procedures, and internal control procedures.
3. Involve business management in the creation of management documentation, and integrate any procedures with existing management and control procedures.
4. Provide training to business management on how to manage the system effectively.
5. Collect regular feedback from business management on the adequacy of the supporting documentation, procedures and related training.

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

Control Practices

1. Create all the required user instructions, documentation, procedures and training materials on a timely basis to enable efficient and effective use of the new system.
2. Create informative and understandable end-user documentation and reference materials, designed for all levels of expertise, written in plain language and easily accessible (e.g., electronic documentation).
3. Involve end-user groups in the creation of end-user support documentation, and integrate any procedures with existing end-user procedures.
4. Provide training to end users on how to use the system effectively.
5. Assess end-user documentation (such as procedure manuals, online help and help desk support material) for content and quality as part of user acceptance testing of the system.
6. Collect regular feedback from end users on the adequacy of the end-user 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

Control Practices

1. Create informative and understandable system maintenance and support documentation that is written in plain language and is easily accessible (e.g., service desk scenarios and electronic documentation).
2. Involve operations and support staff in the creation of maintenance and support documentation, and integrate any procedures with existing operational procedures.
3. Provide training to operations support staff on how to support the new system effectively. Include the business purpose of the system and service levels required.
4. Assess operations documentation (such as procedure manuals, online help, FAQs and help desk support material) for content and quality as part of user acceptance testing of the system.
5. Collect regular feedback from operations and support staff on the adequacy of the operations documentation, procedures and related training.

AI5 Procure IT Resources

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 fulfilling 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

Control Practices

1. Define IT procurement policies and procedures in alignment with the organisation's procurement policies and procedures. The IT procurement policies and procedures should address specific concerns such as:
   - Legislative requirements
   - Compliance with the organisation's IT acquisition policy
   - Involvement of IT legal contract expertise
   - Licensing and leasing requirements
   - Technology upgrade clauses
   - Escrow arrangements
   - Vendor software support and security arrangements
   - Ensuring involvement of the business
   - Total cost of ownership
   - Acquisition plan for major acquisitions
   - Recording of assets
2. Define and implement standard procurement procedures that use selection approaches responsive to the risks associated with the procurement.
3. Define and implement required approvals at key decision points during the procurement processes. Obtain approval from senior management in advance, if the existing policy will not be followed.
4. Record receipt of all hardware and software acquisitions in an asset inventory, and assess the quality before making any payment.

AI5 Procure IT Resources (cont.)

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

Control Practices

1. Establish supplier contract management policies and procedures in accordance with legal terms and conditions. The policies and procedures should address specific concerns such as:
   - Supplier responsibilities
   - Client responsibilities
   - Supplier SLAs
   - Monitoring and reporting against SLAs
   - Transition arrangements
   - Notification and escalation procedures
   - Security standards, records management and control requirements
   - Required supplier QA practices
   - Right to audit
   - Penalties or incentives relating to agreed-upon service levels
   - Intellectual property rights
   - Provision for independent assurance
   - Technology upgrade clauses

   All contracts and contract changes should be reviewed by legal advisors.
2. Define and implement a policy and related procedures to establish, change and terminate supplier contracts. Consult the appropriate stakeholders, including legal, purchasing, audit, business and IT representatives.
3. Perform review of supplier internal controls by management or independent third parties based on contracts with key service suppliers.
4. Obtain and review contracts for clauses relating to third-party reviews and obtain reports from such reviews.
5. When defining the contract remedies, consider software escrow agreements and alternative suppliers or standby agreements in the event of supplier failure.
6. Enquire whether remedies were considered when defining the contract.

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

Control Practices

1. Review all requests for information (RFIs) and requests for proposal (RFPs) to ensure that they:
   - Clearly define requirements
   - Include a procedure to clarify requirements
   - Allow vendors sufficient time to prepare their proposals
   - Clearly define award criteria and the decision process
2. Evaluate RFIs and RFPs in accordance with the approved evaluation process/criteria, and maintain documentary evidence of the evaluations. Verify the references of candidate vendors.
3. Select the supplier that best fits the RFP, document and communicate the decision, and sign the contract.
4. In the specific case of software acquisition, include and enforce the rights and obligations of all parties in the contractual terms. These rights and obligations may include ownership and licencing of intellectual property, maintenance, warranties, arbitration procedures, upgrade terms, and fit for purpose, including security, escrow and access rights.
5. In the specific case of acquisition of development resources, include and enforce the rights and obligations of all parties in the contractual terms. These rights and obligations may include ownership and licencing of intellectual property; fit 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. Obtain legal advice on resource development acquisition agreements regarding ownership and licencing of intellectual property.
6. In the specific case of acquisition of infrastructure, facilities and related services, include and enforce the rights and obligations of all parties in the contractual terms. These rights and obligations may include service levels, maintenance procedures, access controls, security, performance review, basis for payment and arbitration procedures.

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

Control Practices

1. Review the technology delivery life cycle and related deliverables and approve deliverables at key points in the acquisition cycle. Ensure that technology updates are available within agreed-upon time frames.
2. Obtain broad licencing rights and ownership wherever possible and ensure that the supplier is in compliance with applicable regulations.
3. Confirm that the technology acquired delivers as required, proposed and contractually agreed upon, through oversight, inspection and testing. Oversee the delivery of technology components of identified automated solutions. Test acquired software/hardware resources with the standard test procedures, in appropriate environments and using representative data. Maintain test data confidentiality where applicable. Review documentation and knowledge transfer to enable efficient future maintenance.

AI6 Manage Changes

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

Control Practices

1. Develop, document and promulgate a change management framework that specifies the policies and processes, including:
   - Roles and responsibilities
   - Classification and prioritisation of all changes based on business risk
   - Assessment of impact
   - Authorisation and approval of all changes by the business process owners and IT
   - Tracking and status of changes
   - Impact on data integrity (e.g., all changes to data files being made under system and application control rather than by direct user intervention)
2. Establish and maintain version control over all changes.
3. Implement roles and responsibilities that involve business process owners and appropriate technical IT functions. Ensure appropriate segregation of duties.
4. Establish appropriate record management practices and audit trails to record key steps in the change management process. Ensure timely closure of changes. Elevate and report to management changes that are not closed in a timely fashion.
5. Consider the impact of contracted services providers (e.g., of infrastructure, application development and shared services) on the change management process. Consider integration of organisational change management processes with change management processes of service providers. Consider the impact of the organisational change management process on 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

Control Practices

1. Develop a process to allow business process owners and IT to request changes to infrastructure, systems or applications. Develop controls to ensure that all such changes arise only through the change request management process.
2. Categorise all requested changes (e.g., infrastructure, operating systems, networks, application systems, purchased/packaged application software).
3. Prioritise all requested changes. Ensure that the change management process identifies both the business and technical needs for the change. Consider legal, regulatory and contractual reasons for the requested change.
4. Assess all requests in a structured fashion. Ensure that the assessment process addresses impact analysis on infrastructure, systems and applications. Consider security, legal, contractual and compliance implications of the requested change. Consider also interdependencies amongst changes. Involve business process owners in the assessment process, as appropriate.
5. Ensure that each change is formally approved by business process owners and IT technical stakeholders, as appropriate.

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

Control Practices

1. Ensure that a documented process exists within the overall change management process to declare, assess, authorise and record an emergency change.
2. Ensure that emergency changes are processed in accordance with the emergency change element of the formal change management process.
3. Ensure that all emergency access arrangements for changes are appropriately authorised, documented and revoked after the change has been applied.
4. Conduct a post-implementation review of all emergency changes, involving all concerned parties. The review should consider implications for aspects such as further application system maintenance, impact on development and test environments, application software development quality, documentation and manuals, and data integrity.

AI6 Manage Changes (cont.)

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

Control Practices

1. Establish a process to allow requestors and stakeholders to track the status of requests throughout the various stages of the change management process.
2. Categorise change requests in the tracking process (e.g., rejected, approved but not yet initiated, approved and in process, and closed).
3. Implement change status reports with performance metrics to enable management review and monitoring of both the detailed status of changes and the overall state (e.g., aged analysis of change requests). Ensure that status reports form an audit trail so changes can subsequently be tracked from inception to eventual disposition.
4. Monitor open changes to ensure that all approved changes are closed in a timely fashion, depending on priority.

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

Control Practices

1. Ensure that documentation—including operational procedures, configuration information, application documentation, help screens and training materials—follows the same change management procedure and is considered to be an integral part of the change.
2. Consider an appropriate retention period for change documentation and pre- and post-change system and user documentation.
3. Update business processes for changes in hardware or software to ensure that new or improved functionality is used.
4. Subject documentation to the same level of testing as the actual change.

AI7 Install and Accredit Solutions and Changes

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

Control Practices

1. For systems development, implementation or modification projects, a training plan is an integral part of the overall project master plan. Ensure that the plan clearly identifies learning objectives, resources, key milestones, dependencies and critical path tasks impacting the delivery of the training plan. The plan should consider alternative training strategies depending on the business needs, risk level (e.g., for mission-critical systems, a formal system of user accreditation and reaccreditation may be appropriate), and regulatory and compliance requirements (e.g., impact of varying privacy laws may require adaptation of the training at a national level).
2. Ensure that the training plan identifies and addresses all impacted groups, including business end users, IT operations, support and IT application development training, and service providers. The training plan should incorporate the delivery of the training in a timely manner. It should also identify staff members who must be trained and those for whom training is desirable.
3. Consider alternative training strategies that satisfy the training requirements, and select the most cost-effective approach that aligns with the organisation's training framework. Alternative strategies include train the trainer, end-user accreditation and intranet-based training.
4. Confirm that there is a process to ensure that the training plan is executed satisfactorily. Complete the documentation detailing compliance with the training plan. Examples of information include lists of staff members invited to attend the training, attendees, evaluations of achievement of learning objectives and other feedback.
5. Monitor training to obtain feedback that could lead to potential improvements in either the training or the system.
6. Monitor all planned changes to ensure that training requirements have been considered and suitable plans created. Consider postponing the change if training has not been performed and the lack of training would jeopardise the implementation of the change.

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

Control Practices

1. Develop and document the test plan, which aligns to the project quality plan and relevant organisational standards. Communicate and consult with appropriate business process owners and IT stakeholders.
2. Ensure that the test plan reflects an assessment of risks from the project and that all functional and technical requirements are tested. Based on assessment of the risk of system failure and faults on implementation, the plan should include requirements for performance, stress, usability, pilot and security testing.
3. Ensure that the test plan addresses the potential need for internal or external accreditation of outcomes of the test process (e.g., financial regulatory requirements).
4. Ensure that the test plan identifies necessary resources to execute testing and evaluate the results. Examples of resources include construction of test environments and staff for the test group, including potential temporary replacement of test staff in the production or development environments. Ensure that stakeholders are consulted on the resource implications of the test plan.
5. Ensure that the test plan identifies testing phases appropriate to the operational requirements and environment. Examples of such testing phases include unit test, system test, integration test, user acceptance test, performance test, stress test, data conversion test, security test, operational readiness, and backup and recovery tests.
6. Confirm that the test plan considers test preparation (including site preparation), training requirements, installation or an update of a defined test environment, planning/performing/documenting/retaining test cases, error and problem handling, correction and escalation, and formal approval.
7. Ensure that the test plan establishes clear criteria for measuring the success of undertaking each testing phase. Consult the business process owners and IT stakeholders in defining the success criteria. Determine that the plan establishes remediation procedures when the success criteria are not met (e.g., in a 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).
8. Confirm that all test plans are approved by stakeholders, including business process owners and IT, as appropriate. Examples of such 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

Control Practices

1. Define a policy for numbering and frequency of releases.
2. Confirm that all implementation plans are approved by stakeholders, including technical and business.
3. Create an implementation plan reflecting the outcomes of a formal review of technical and business risks. Include with the implementation plan:
   - The broad implementation strategy
   - The sequence of implementation steps
   - Resource requirements
   - Interdependencies
   - Criteria for management agreement to the production implementation
   - Installation verification requirements
   - Transition strategy for production support

   Align the implementation plan with the business change management plan.
4. Obtain commitment from third parties to their involvement in each step of the implementation.
5. Identify and document the fallback and recovery process.

AI7 Install and Accredit Solutions and Changes (cont.)

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

Control Practices

1. Ensure that the test environment is representative of the future operating landscape, including likely workload stress, operating systems, necessary application software, database management systems, and network and computing infrastructure found in the production environment.
2. Ensure that the test environment is secure and incapable of interacting with production systems.
3. Create a database of test data that are representative of the production environment. Sanitise data used in the test environment from the production environment according to business needs and organisational standards (e.g., consider whether compliance or regulatory requirements oblige the use of sanitised data).
4. Protect sensitive test data and results against disclosure, including access, retention, storage and destruction. Consider the effect of interaction of organisational systems with those of third parties.
5. Put in place a process to enable proper retention or disposal of test results, media and other associated documentation to enable adequate review and subsequent analysis as required by the test plan. Consider the effect of regulatory or compliance requirements.

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

Control Practices

1. Define a data conversion and infrastructure migration plan. Consider, for example, hardware, networks, operating systems, software, transaction data, master files, backups and archives, interfaces with other systems (both internal and external), procedures and system documentation, in the development of the plan.
2. Ensure that the data conversion plan incorporates methods for collecting, converting and verifying data to be converted, and identifying and resolving any errors found during conversion. This includes comparing the original and converted data for completeness and integrity.
3. Confirm that the data conversion plan does not require changes in data values unless absolutely necessary for business reasons. Document changes made to data values, and secure approval from the business process data owner.
4. Consider real-time disaster recovery, business continuity planning, and reversion in the data conversion and infrastructure migration plan where risk management, business needs, or regulatory/compliance requirements demand.
5. Co-ordinate and verify the timing and completeness of the conversion cutover so there is a smooth, continuous transition with no loss of transactions. Where necessary, in the absence of any other alternative, freeze live operations.
6. Ensure that there is a backup of all systems and data taken at the point prior to conversion, audit trails are maintained to enable the conversion to be retraced, and there is a fallback and recovery plan in case the conversion fails. Ensure that retention of backup and archived data conforms to business needs and regulatory or compliance requirements.

AI7 Install and Accredit Solutions and Changes (cont.)

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

Control Practices

1. Ensure that testing of changes is undertaken in accordance with the testing plan. Ensure that the testing is designed and conducted by a test group independent from the development team. Consider the extent to which business process owners and end users are involved in the test group. Ensure that testing is conducted only within the test environment.
2. Ensure that the tests and anticipated outcomes are in accordance with the defined success criteria set out in the testing plan.
3. Consider using clearly defined test instructions (scripts) to implement the tests. Ensure that the independent test group assesses and approves each test script to confirm that it adequately addresses test success criteria set out in the test plan. Consider using scripts to verify the extent to which the system meets security requirements. Consider the appropriate balance between automated scripted tests and interactive user testing.
4. Undertake tests of security in accordance with the test plan. Measure the extent of security weaknesses or loopholes. Consider the effect of security incidents since construction of the test plan. Consider the effect on access and boundary controls.
5. Undertake tests of system and application performance in accordance with the test plan. Consider a range of performance metrics (e.g., end-user response times and database management system update performance).
6. When undertaking testing, ensure that the fallback and rollback elements of the test plan have been addressed.
7. Identify, log and classify (e.g., minor, significant and mission-critical) errors during testing. Ensure that an audit trail of test results is available. Communicate results of testing to stakeholders in accordance with the test plan to facilitate bug fixing and further quality enhancement.

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

Control Practices

1. Ensure that the scope of final acceptance evaluation activities covers all components of the information system (e.g., application software, facilities, technology, user procedures, operations procedures, monitoring and support).
2. Ensure that the categorised log of errors found in the testing process has been addressed by the development team. Ensure that the cause of errors has been remediated (e.g., by appropriate changes to the application, configuration or workaround, and/or delayed correction where the error is minor).
3. Ensure that the final acceptance evaluation is measured against the success criteria set out in the testing plan. Ensure that the review and evaluation process is appropriately documented.
4. Document and interpret the final acceptance testing results, and present them in a form that is understandable to business process owners and IT so an informed review and evaluation can take place.
5. Ensure that business process owners, third parties (as appropriate) and IT stakeholders formally sign off on the outcome of the testing process as set out in the testing plan. Such approval is mandatory prior to promotion to production.

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

Control Practices

1. Ensure that a formal process for application, system and configuration transfer from testing to the production environment exists. Ensure that the process is in accordance with organisational change management standards.
2. Ensure that the approval process clearly identifies effective dates for promotion to production of new systems, applications or infrastructure, as appropriate. Ensure that the approval process clearly identifies effective dates for retirement of old systems, applications or infrastructure, as appropriate.
3. Ensure 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).
4. Consider the extent of parallel processing of the old and new system in line with the implementation plan.
5. Promptly update all copies of system documentation and configuration information, including backup copies stored offsite, for software, hardware, operating personnel and system users before a new or modified system is implemented. Promptly update relevant contingency plan documents, as appropriate.
6. Ensure that all source program libraries are updated promptly with the version of the program being transferred from testing to the production environment. Ensure that the existing version and its supporting documentation are archived. Ensure that promotion to production of systems, application software and infrastructure is under configuration control.
7. In high-risk environments, consider obtaining from the testing function the media used for implementation to ensure that the software implemented is unchanged from what has been tested.
8. Where distribution of systems or application software is conducted electronically, control automated software distribution to ensure that users are notified and distribution occurs only to authorised and correctly identified destinations. Implement checks in the distribution process to verify that the destination environment is of the correct standard implementation and version prior to the new software being installed and to ensure implementation on the approved effective date. Include in the release process backout procedures to enable the distribution of software changes to be reviewed in the event of a malfunction or error.
9. Where distribution takes physical form, keep a formal log of what software and configuration items have been distributed, to whom, where they have been implemented, and when each has been updated. Implement a procedure to ensure the log's integrity and completeness. Ensure that there are checks in the physical distribution process to ensure implementation on the approved effective date.
10. Update all program copies in use in the production environment with the version being transferred from testing to the production environment in accordance with the implementation plan.

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

Control Practices

1. Establish procedures to ensure that post-implementation reviews 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 have occurred
   - Key risks are mitigated
   - The change management, installation and accreditation processes were performed effectively and efficiently
2. Consult business process owners and IT technical management in the choice of metrics for measurement of success and achievement of requirements and benefits.
3. Ensure that the form of the post-implementation review is in accordance with the organisational change management process. Involve business process owners and third parties, as appropriate.
4. Consider requirements for post-implementation review arising from outside business and IT (e.g., internal audit, enterprise risk management, regulatory compliance).
5. Agree on and implement an action plan to address issues identified in the post-implementation review. Involve business process owners and IT technical management in the development of the action plan.

DS—Deliver and Support

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

CONTROL PRACTICES

DS1 Define and Manage Service Levels

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

Control Practices

1. Define and document an SLA framework to manage the IT service life cycle. The process should involve senior management representing both the business and IT functions. The framework should identify IT objectives and specify measures of IT performance in meeting business objectives. The respective roles of the business and internal and external service providers should be clearly articulated. Complement the framework with formally defined and approved qualitative and quantitative measures that are easily understood and achievable.
2. Create a service catalogue that incorporates service requirements, service definitions, SLAs, OLAs and funding sources.
3. Put in place a process to continually realign SLA objectives and performance measures with business objectives and IT strategy, leveraging subject experts and comparing to accepted industry practice and benchmarks.
4. Define and implement procedures for monitoring and reporting service level performance measures. Establish escalation and resolution methods for service level issues.
5. Establish and implement an appropriate change management process for the framework, service catalogue, SLA objectives and performance measures.
6. Define a service improvement programme.

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

Control Practices

1. Define a process for developing, reviewing, approving and adjusting the service catalogue or portfolio of services based on service characteristics and business requirements.
2. Put in place a management process to ensure that the service catalogue or portfolio is available, complete and up to date, and is periodically reviewed to ensure alignment with business requirements.

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

Control Practices

1. Ensure that the stakeholders from IT and the business negotiate, agree to and approve service requirements, and document and communicate their SLA as appropriate. The format and contents include exclusions, commercial arrangements and OLAs.
2. Confirm that the SLA management process promotes, promulgates, measures (qualitative and quantitative) and monitors the SLA objectives.
3. Perform periodic reviews of the SLA objectives, effectiveness and efficiency, and report to the SLA stakeholders.
4. Improve or adjust SLAs based on performance feedback and changes to customer and business requirements.

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

Control Practices

1. Define a process to develop, manage, review and adjust OLAs.
2. Ensure that OLAs are in place that identify, document and explain how the services will be technically delivered to support the SLA(s). Ensure that the OLAs specify all the technical processes that are utilised and the SLAs they support (a single OLA may support several SLAs).

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 • Disatisfied users due to lack of information, irrespective of quality of service

Control Practices

1. Define a process to continuously monitor all agreed-upon service levels.
2. Provide regular and formal reporting of SLA performance, including deviations from the agreed-upon values, and distribute this report to different levels in the organisation.
3. Perform regular reviews to forecast and identify 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

Control Practices

1. Put in place a process, outlined within the service level framework, to assess and report service level performance and ensure that the agreements and UCs are effective, efficient and up to date.
2. Conduct reviews of SLAs and UCs on a regular basis with all impacted parties to ensure that they remain effective and are in alignment with business objectives.

DS2 Manage Third-party Services

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 miscommunciations, poor services and increased costs

Control Practices

1. Define and regularly review criteria to identify and categorise all supplier relationships according to the supplier type, significance and criticality of service. The list should include a category describing vendors as preferred, non-preferred or not recommended.
2. Establish and maintain a detailed register of suppliers, including name, scope, purpose of the service, expected deliverables, service objectives and key contact details.

DS2 Manage Third-party Services

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 responsibiltiies between customer and supplier	• Supplier not responsive or committed to the relationship • Problems and issues not resolved • Inadequate service quality

Control Practices

1. Define and formalise roles and responsibilities for each service supplier.
2. Assign relationship owners for all suppliers and make them accountable for the quality of service(s) provided.
3. Document the supplier relationship managers and communicate the information within the organisation.
4. Establish and document a formal communication process between the organisation and the service provider.
5. Ensure that contracts with key service suppliers provide for a review of supplier internal controls by management or independent third parties.
6. Regularly review the reports between the organisation and the service supplier.
7. Register incidents caused by suppliers and report them using the company's internal incident management process.
8. Periodically review and assess supplier performance against established and agreed-upon service levels. Clearly communicate suggested changes to the service supplier.

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 • Indentification 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

Control Practices

1. Identify and monitor supplier risks in accordance with the organisation's established risk management process.
2. Identify and document in the contract supplier risks (and remedies) associated with the supplier's inability to fulfil the contractual agreement(s).
3. When defining the contract, consider remedies including software escrow agreements, alternative suppliers or standby agreements in the event of supplier failure.
4. Review all contracts for legal and regulatory requirements.

DS2 Manage Third-party Services (cont.)

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

Control Practices

1. Define and document criteria to monitor service suppliers' performance.
2. Ensure that the supplier regularly reports on agreed-upon performance criteria.
3. Invite users to provide feedback for assessment of supplier performance and quality of service.
4. Evaluate the costs and market conditions for the service levels by benchmarking against alternative suppliers, and identify potential for improvement.
5. Define arbitration procedures to consult an arbitration committee before bringing an action.

DS3 Manage Performance and Capacity

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

Control Practices

1. Define a process and framework for developing, reviewing and adjusting the performance and capacity plan.
2. Consider the following (current and forecasted) in the development of the performance and capacity plan:
   - Customer requirements
   - Business priorities
   - Business objectives
   - Budget impact
   - Resource utilisation
   - IT capabilities and industry trends, including:
     – Application performance
     – Technology, availability and reliability
     – Performance, capacity and support to users
     – Continuity and contingency planning
     – Data privacy and security considerations
3. Develop and maintain the performance and capacity plan in a timely manner, and ensure that it is documented and agreed to by the stakeholders, aligned to SLAs, and properly recorded.

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

Control Practices

1. Monitor actual performance and capacity usage against defined thresholds, supported where necessary with automated software.
2. Identify and follow up on all incidents caused by inadequate performance or capacity.
3. Regularly evaluate the current levels of performance for all processing levels (business demand, service capacity and resource capacity) by comparing them against trends and SLAs, taking into account changes in the environment.

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

Control Practices

1. Use appropriate sizing and capacity monitoring and modelling tools and techniques to measure and estimate capacity and performance.
2. Measure performance and capacity, compare the results to baselines and models (qualitatively and quantitatively), and then compare them with the forecast at intervals determined by the trends.
3. Adjust the performance and capacity plans and SLAs based on realistic, new, proposed and/or projected business and IT changes as well as reviews of actual performance and capacity usage, including workload levels.
4. Ensure that management performs comparisons of actual demand on IT resources with forecasted supply and demand to evaluate current forecasting techniques and make improvements where possible.

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

Control Practices

1. Obtain guidance from vendor product manuals to ensure an appropriate level of performance availability for peak processing and workloads.
2. Identify performance and capacity gaps based on monitoring current and forecasted performance. Use the known availability, continuity and recovery specifications (AI2) to classify IT resources and allow prioritisation.
3. Define corrective actions, e.g., shifting workload, prioritising tasks or adding system (or other) resources, when performance and capacity issues are identified.
4. Integrate required corrective actions into the capacity plan, and feed them into the appropriate planning processes (information architecture and technological direction) and change management process.
5. Define an escalation procedure for swift resolution in case of emergency capacity and performance problems.

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

Control Practices

1. Establish a process for gathering data to provide management with monitoring and reporting information for availability, performance and capacity workload of all IT resources.
2. Provide regular reporting of the results in an appropriate form for review by IT and business management and communication to enterprise management.
3. Ensure that the monitoring and reporting activities are integrated in the iterative capacity management activities (monitoring, analysis, tuning and implementation).
4. Ensure that capacity reports are fed into the budgeting processes.

DS4 Ensure Continuous Service

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

Control Practices

1. Assign responsibility for and establish an enterprisewide business continuity management process. This process should include an IT continuity framework to ensure that a business impact analysis (BIA) is completed and IT continuity plans support business strategy, a prioritised recovery strategy, necessary operational support based on these strategies and any compliance requirements.
2. Ensure that the continuity framework includes:
   - The conditions and responsibilities for activating and/or escalating the plan
   - Prioritised recovery strategy, including the necessary sequence of activities
   - Minimum recovery requirements to maintain adequate business operations and service levels with diminished resources
   - Emergency procedures
   - Fallback procedures
   - Temporary operational procedures
   - IT processing resumption procedures
   - Maintenance and test schedule
   - Awareness, education and training activities
   - Responsibilities of individuals
   - Regulatory
   - Critical assets and resources and up-to-date personnel contact information needed to perform emergency, fallback and resumption procedures
   - Alternative processing facilities as determined within the plan
   - Alternative suppliers for critical resources
   - Chain of communications plan
   - Key resources identified
3. Ensure that the IT continuity framework addresses:
   - Organisational structure for IT continuity management as a liaison to organisational continuity management
   - Roles, tasks and responsibilities defined by SLAs and/or contracts for internal and external service providers
   - Documentation standards and change management procedures for all IT continuity-related procedures and tests
   - Policies for conducting regular tests
   - The frequency and conditions (triggers) for updating the IT continuity plans
   - The results of the risk assessment process (PO9)

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

Control Practices

1. Create an IT continuity plan, including:
   - The conditions and responsibilities for activating and/or escalating the plan
   - Prioritised recovery strategy, including the necessary sequence of activities
   - Minimum recovery requirements to maintain adequate business operations and service levels with diminished resources
   - Emergency procedures
   - Fallback procedures
   - Temporary operational procedures
   - IT processing resumption procedures
   - Maintenance and test schedule
   - Awareness, education and training activities
   - Responsibilities of individuals
   - Regulatory requirements
   - Critical assets and resources and up-to-date personnel contact information needed to perform emergency, fallback and resumption procedures
   - Alternative processing facilities as determined within the plan
   - Alternative suppliers for critical resources
2. Define underlying assumptions (e.g., level of outage covered by the plan) in the IT continuity plan and which systems (i.e., computer systems, network components and other IT infrastructure) and sites are to be included. Note alternative processing options for each site.
3. Ensure that the IT continuity plan includes a defined checklist of recovery events as well as a form for event logging.
4. Establish and maintain detailed information for every recovery site, including assigned staff and logistics (e.g., transport of media to the recovery site). This information should include:
   - Processing requirements for each site
   - Location
   - Resources (e.g., systems, staff, support) available at each location
   - Utility companies on which the site depends
5. Define response and recovery team structures, including reporting requirements roles and responsibilities as well as knowledge, skills and experience requirements for all team members. Include contact details of all team members, and ensure that that they are maintained and readily available (e.g., offsite team, backup managing team).
6. Define and prioritise communication processes and define responsibility for communication (e.g., public, press, government). Maintain contact details of relevant stakeholders (e.g., crisis management team, IT recovery staff, business stakeholders, staff), service providers (e.g., vendors, telecommunications provider) and external parties (e.g., business partners, media, government bodies, public).
7. Maintain procedures to protect and restore the affected part of the organisation, including, where necessary, reconstruction of the affected site or its replacement. This also includes procedures to respond to further disasters while in the backup site.
8. Create emergency procedures to ensure the safety of all affected parties, including coverage of occupational health and safety requirements (e.g., counselling services) and co-ordination with public authorities.

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

Control Practices

1. Define priorities for all applications, systems and sites that are in line with business objectives. Include these priorities in the continuity plan. When defining priorities, consider:
   - Business risk and IT operational risk
   - Interdependencies
   - The data classification framework
   - SLAs and OLAs
   - Costs
2. Consider resilience, response and recovery requirements for different tiers, e.g., one to four hours, four to 24 hours, more than 24 hours and critical business operational periods.

DS4 Ensure Continuous Service (cont.)

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

Control Practices

1. Maintain a change history of the IT continuity plan. Ensure proper version management of the plan, e.g., through the use of document management systems. Ensure that all distributed copies are the same version.
2. Involve the business continuity and IT continuity manager(s) in the change management processes to ensure awareness of important changes that would require updates to the IT continuity plans.
3. Update the IT continuity plan as described by the IT continuity framework. Triggering events for the update of the plan include:
   - Important architecture changes
   - Important business changes
   - Key staff changes or organisation changes
   - Incidents/disasters and the lessons learnt
   - Results from continuity plan tests

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

Control Practices

1. Schedule IT continuity tests on a regular basis or after major changes in the IT infrastructure or to the business and related applications. Ensure that all new components (e.g., hardware, software updates, new business processes) are included in the schedule.
2. Create a detailed test schedule based on established recovery priorities. Ensure that test scenarios are realistic. Tests should include recovery of critical business application processing and should not be limited to recovery of infrastructure. Make sure that testing time is adequate and will not impact the ongoing business.
3. Establish an independent test task force that keeps track of all events and records all results to be discussed in the debriefing. The members of the task force should not be key personnel defined in the plan. This task force should independently report to senior management and/or the board of directors.
4. Perform a debriefing event wherein all failures are analysed and solutions are developed or handed over to task forces. Ensure that all outstanding issues related to continuity planning are analysed and resolved in an appropriate time frame. Schedule a retesting of the changes using similar or stronger parameters to ensure a positive impact on the recovery procedures.
5. If testing is not feasible, evaluate alternative means for ensuring resources for business continuity (e.g., dry run).
6. Measure and report the success or failure of the test and, therefore, the continuity and contingency ability for services to the risk management process (PO9).

DS4 Ensure Continuous Service (cont.)

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

Control Practices

1. On a regular basis (at least annually) or upon plan changes, provide training to the required staff members with respect to their roles and responsibilities.
2. Assess all needs for training periodically and update all schedules appropriately. While planning the training, take into account the timing and the extent of plan updates and changes, turnover of recovery staff, and recent test results.
3. Perform regular IT continuity awareness programmes for all level of employees as well as IT stakeholders to increase awareness of the need for an IT continuity strategy and their key role within it.
4. Measure and document training attendance, training results and coverage.

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

Control Practices

1. Define a proper distribution list for the IT continuity plan and keep this list up to date. Include people and locations in the list on a need-to-know basis. Ensure that procedures exist with instructions for storage of confidential information.
2. Define a distribution process that:
   - Distributes the IT continuity plan in a timely manner to all recipients and locations on the distribution list
   - Collects and destroys obsolete copies of the plan in line with the organisation's policy for discarding confidential information
3. Ensure that all digital and physical copies of the plan are protected in an appropriate manner (e.g., encryption, password protection) and the document is accessible only by authorised personnel (recovery staff).

DS4 Ensure Continuous Service (cont.)

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

Control Practices

1. Activate the IT continuity plan when conditions require it.
2. Maintain an activity and problem log during recovery activities to be used during post-resumption review.

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

Control Practices

1. Provide protection for data commensurate with the value and security classification, from the time they are taken offsite, while in transport to/from the organisation and at the storage location.
2. Ensure that the backup facilities are not subject to the same risks (e.g., geography, weather, key service provider) as the primary site.
3. Perform regular testing of:
   - The quality of the backups and media
   - The ability to meet the committed recovery time frame
4. Ensure that the backups contain all data, programs and associated resources needed for recovery according to plan.
5. Provide sufficient recovery instructions and adequate labelling of backup media.
6. Maintain an inventory of all backups and backup media. Ensure inclusion of all departmental processing, if applicable.

DS4 Ensure Continuous Service (cont.)

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

Control Practices

1. Using the problem and activity log of recovery activities, identify the shortcomings of the plan after re-establishing normal processing, and agree on opportunities for improvement to include in the next update of the IT continuity plan.

DS5 Ensure Systems Security

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

Control Practices

1. Define a charter for IT security, defining for the security management function:
   - Scope and objectives for the security management function
   - Responsibilities
   - Drivers (e.g., compliance, risk, performance)
2. Confirm that the board, executive management and line management direct the policy development process to ensure that the IT security policy reflects the requirements of the business.
3. Set up an adequate organisational structure and reporting line for information security, ensuring that the security management and administration functions have sufficient authority. Define the interaction with enterprise functions, particularly the control functions such as risk management, compliance and audit.
4. Implement an IT security management reporting mechanism, regularly informing the board and business and IT management of the status of IT security so that appropriate management actions can be taken.

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

Control Practices

1. Define and maintain an overall IT security plan that includes:
   - 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
2. Collect information security requirements from IT tactical plans (PO1), data classification (PO2), technology standards (PO3), security and control policies (PO6), risk management (PO9), and external compliance requirements (ME3) for integration into the overall IT security plan.
3. Translate the overall IT security plan into enterprise information security baselines for all major platforms and integrate it into the configuration baseline (DS9).
4. Provide information security requirements and implementation advice to other processes, including the development of SLAs and OLAs (DS1 and DS2), automated solution requirements (AI1), application software (AI2), and IT infrastructure components (AI3).
5. Communicate to all stakeholders and users in a timely and regular fashion on updates of the information security strategy, plans, policies and procedures.

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

Control Practices

1. Establish and communicate policies and procedures to uniquely identify, authenticate and authorise access mechanisms and access rights for all users on a need-to-know/need-to-have basis, based on predetermined and preapproved roles. Clearly state accountability of any user for any action on any of the systems and/or applications involved.
2. Ensure that roles and access authorisation criteria for assigning user access rights take into account:
   - Sensitivity of information and applications involved (data classification)
   - Policies for information protection and dissemination (legal, regulatory, internal policies and contractual requirements)
   - Roles and responsibilities as defined within the enterprise
   - The need-to-have access rights associated with the function
   - Standard but individual user access profiles for common job roles in the organisation
   - Requirements to guarantee appropriate segregation of duties
3. Establish a method for authenticating and authorising users to establish responsibility and enforce access rights in line with sensitivity of information and functional application requirements and infrastructure components, and in compliance with applicable laws, regulations, internal policies and contractual agreements.
4. Define and implement a procedure for identifying new users and recording, approving and maintaining access rights. This needs to be requested by user management, approved by the system owner and implemented by the responsible security person.
5. Ensure that a timely information flow is in place that reports changes in jobs (i.e., people in, people out, people change). Grant, revoke and adapt user access rights in co-ordination with human resources and user departments for users who are new, who have left the organisation, or who have changed roles or jobs.

DS5 Ensure Systems Security (cont.)

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

Control Practices

1. Ensure that access control procedures include but are not limited to:
   - Using unique user IDs to enable users to be linked to and held accountable for their actions
   - Awareness that the use of group IDs results in the loss of individual accountability and are permitted only when justified for business or operational reasons and compensated by mitigating controls. Group IDs must be approved and documented.
   - Checking that the user has authorisation from the system owner for the use of the information system or service, and the level of access granted is appropriate to the business purpose and consistent with the organisational security policy
   - A procedure to require users to understand and acknowledge their access rights and the conditions of such access
   - Ensuring that internal and external service providers do not provide access until authorisation procedures have been completed
   - Maintaining a formal record, including access levels, of all persons registered to use the service
   - A timely and regular review of user IDs and access rights
2. Ensure that management reviews or reallocates user access rights at regular intervals using a formal process. User access rights should be reviewed or reallocated after any job changes, such as transfer, promotion, demotion or termination of employment. Authorisations for special privileged access rights should be reviewed independently at more frequent intervals.

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

Control Practices

1. Implement monitoring, testing, reviews and other controls to:
   - Promptly prevent/detect errors in the results of processing
   - Promptly identify attempted, successful and unsuccessful security breaches and incidents
   - Detect security events and thereby prevent security incidents by using detection and prevention technologies
   - Determine whether the actions taken to resolve a breach of security are effective
2. Conduct effective and efficient security testing procedures at regular intervals to:
   - Verify that identity management procedures are effective
   - Verify that user account management is effective
   - Validate that security-relevant system parameter settings are defined correctly and are in compliance with the information security baseline
   - Validate that network security controls/settings are configured properly and are in compliance with the information security baseline
   - Validate that security monitoring procedures are working properly
   - Consider, where necessary, obtaining expert reviews of the security perimeter

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

Control Practices

1. Describe what a security incident is considered to be. Document within the characteristics a limited number of impact levels to allow commensurate response. Communicate and distribute this information, or relevant parts thereof, to identified people who need to be notified.
2. Ensure that security incidents and appropriate follow-up actions, including root cause analysis, follow the existing incident and problem management processes.
3. Define measures to protect confidentiality of information related to security incidents.

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

Control Practices

1. Ensure that all hardware, software and facilities related to the security function and controls, e.g., security tokens and encryptors, are tamperproof.
2. Secure security documentation and specifications to prevent unauthorised access. However, do not make security of systems reliant solely on secrecy of security specifications.
3. Make the security design of dedicated security technology (e.g., encryption algorithms) strong enough to resist exposure, even if the security design is made available to unauthorised individuals.
4. Evaluate the protection mechanisms on a regular basis (at least annually) and perform updates to the protection of the security technology, if necessary.

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

Control Practices

1. Ensure that there are appropriate procedures and practices in place for the generation, storage and renewal of the root key, including dual custody and observation by witnesses.
2. Make sure that procedures are in place to determine when a root key renewal is required (e.g., the root key is compromised or expired).
3. Create and maintain a written certification practice statement that describes the practices that have been implemented in the certification authority, registration authority and directory when using a public-key-based encryption system.
4. Create cryptographic keys in a secure manner. When possible, enable only individuals not involved with the operational use of the keys to create the keys. Verify the credentials of key requestors (e.g., registration authority).
5. Ensure that cryptographic keys are distributed in a secure manner (e.g., offline mechanisms) and stored securely, that is:
   - In an encrypted form regardless of the storage media used (e.g., write-once disk with encryption)
   - With adequate physical protection (e.g., sealed, dual custody vault) if stored on paper
6. Create a process that identifies and revokes compromised keys. Notify all stakeholders as soon as possible of the compromised key.
7. Verify the authenticity of the counterparty before establishing a trusted path.

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

Control Practices

1. Establish, document, communicate and enforce a malicious software prevention policy in the organisation. Ensure that people in the organisation are aware of the need for protection against malicious software, and their responsibilities relative to same.
2. Install and activate malicious software protection tools on all processing facilities, with malicious software definition files that are updated as required (automatically or semi-automatically).
3. Distribute all protection software centrally (version and patch-level) using centralised configuration and change management.
4. Regularly review and evaluate information on new potential threats.
5. Filter incoming traffic, such as e-mail and downloads, to protect against unsolicited information (e.g., spyware, phishing e-mails).

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

Control Practices

1. Establish, maintain, communicate and enforce a network security policy (e.g., provided services, allowed traffic, types of connections permitted) that is reviewed and updated on a regular basis (at least annually).
2. Establish and regularly update the standards and procedures for administering all networking components (e.g., core routers, DMZ, VPN switches, wireless).
3. Properly secure network devices with special mechanisms and tools (e.g., authentication for device management, secure communications, strong authentication mechanisms). Implement active monitoring and pattern recognition to protect devices from attack.
4. Configure operating systems with minimal features enabled (e.g., features that are necessary for functionality and are hardened for security applications). Remove all unnecessary services, functionalities and interfaces (e.g., graphical user interface [GUI]). Apply all relevant security patches and major updates to the system in a timely manner.
5. Plan the network security architecture (e.g., DMZ architectures, internal and external network, IDS placement and wireless) to address processing and security requirements. Ensure that documentation contains information on how traffic is exchanged through systems and how the structure of the organisation's internal network is hidden from the outside world.
6. Subject devices to reviews by experts who are independent of the implementation or maintenance of the devices.

DS5 Ensure Systems Security (cont.)

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

Control Practices

1. Determine by using the established information classification scheme how the data should be protected when exchanged.
2. Apply appropriate application controls to protect the data exchange.
3. Apply appropriate infrastructure controls, based on information classification and technology in use, to protect the data exchange.

DS6 Identify and Allocate Costs

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

Control Practices

1. Define and clearly document distinct IT services to support appropriate allocation of costs.
2. Map the IT services to the IT infrastructure.
3. Map the IT services to the business processes and owners that use them.

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

Control Practices

1. Ensure that cost elements adequately capture IT service provision.
2. Inspect the enterprise cost accounting system setup to ensure that all defined IT cost elements are appropriately captured in line with the enterprise's cost accounting models.
3. Ensure that all captured costs are allocated within the IT service function and the business in line with the enterprise's cost accounting models.
4. Ensure that changes in cost structures and business needs are identified and that budgets and forecasts are revised as required.
5. Provide regular management reporting on IT costs to business and IT management. Analyse variances between budgets and forecasts and actual costs.

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

Control Practices

1. Categorise all IT costs appropriately as direct, indirect and overhead, in line with the enterprise management accounting framework.
2. Inspect service definition catalogues to identify services subject to user chargeback and those that are shared services.
3. Define and agree on a model that:
   - Supports the calculation of chargeback rates per service
   - Defines how IT costs will be calculated/charged
   - Is differentiated where and when appropriate
   - Is aligned with the IT budget
4. Design the cost model so it is transparent enough to allow for:
   - Users to identify their actual usage and charges
   - Better predictability of IT costs
   - Efficient and effective utilisation of IT resources
5. After review with user departments, obtain appproval and communicate the IT costing model inputs and outputs to the management of user departments.

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

Control Practices

1. Review the cost/recharge model on a regular basis. Ensure that the enterprise management accounting framework, current business requirements, and changes in the IT services and costs are reflected in the cost/recharge model.
2. Communicate changes in the cost/recharge model with business process owners.
3. Follow up enquires due to unclear cost or pricing procedures immediately. Capture a summary of enquires to further improve the cost/recharge model.

DS7 Educate and Train Users

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

Control Practices

1. Implement a process to identify predetermined requirements (such as for certifications) and/or create competency requirements for user roles, and use this to plan training curriculum for all target groups of users. The process ensures that training and education support compliance with business policies while providing and supporting the employee's career path.
2. Maintain a skills database that contains a gap analysis between the skills required by users and internal providers of technology and the skills and knowledge available. This database should also include competency profiles and records of any skills certifications obtained by users.
3. Incorporate technology training needs into the users' individual performance plans.
4. Implement a process to compile and analyse information from the service desk and identify training requirements.

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

Control Practices

1. Implement a process based on business requirements and support of business to define effective training programmes, and deliver programmes in a timely manner based on identified needs, delivery mechanisms (e.g., classroom, computer-based) and qualifications of trainers.
2. Monitor and record attendance to and completion of training and education programmes. Take appropriate action if individuals do not complete required training for their role.
3. Capture participant and trainer feedback upon completion of training. Incorporate feedback into the process for evaluating training programmes and training delivery mechanisms.

DS7 Educate and Train Users (cont.)

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

Control Practices

1. Test the users' understanding of the training session content after the sessions are completed to measure the understanding of the training received.
2. Summarise and analyse evaluation forms completed after the education and training sessions to measure the quality and relevance of the content and the level of participant satisfaction.
3. Obtain stakeholder feedback to determine the level of satisfaction with the education and training provided.
4. For predetermined timelines, determine measures and capture and assess performance information (e.g., reduced help desk calls, increased productivity of users) that may indicate whether training had the intended impact.
5. Evaluate collected measurements to identify and implement updates to the existing training plan.

DS8 Manage Service Desk and Incidents

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

Control Practices

1. Establish a service desk as a single, initial point of contact for the reporting, monitoring, escalation and resolution of customer requests and incidents. Develop business requirements for the service desk, based on service definitions and SLAs, including hours of operation and expected response time to a call. Ensure that service desk requirements include identifying staffing, tools and integration with other processes, such as change management and problem management.
2. Ensure that there are clear instructions for service desk staff when a request cannot be immediately resolved by service desk personnel. Establish time thresholds to determine when escalation should occur based on the categorisation/prioritisation of the request or incident.
3. Implement the necessary support software and tools (e.g., incident management, knowledge management, incident escalation systems, automated call monitoring) required for operation of the service desk and configured in accordance with SLA requirements, to facilitate automated prioritisation of incidents and rapid resolution.
4. Advise customers of the existence of the service desk and the standards of service they can expect. Obtain user feedback on a regular basis to ensure customer satisfaction and confirm the effectiveness of the service desk operation.
5. Using the service desk software, create service desk performance reports to enable performance monitoring and continuous improvement of the service desk.

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

Control Practices

1. Define priority levels through consultation with the business to ensure that events that are not part of standard operations (incidents) are handled in a timely manner according to the agreed-upon SLAs. Define priority levels on the business impact and urgency. Establish time thresholds to determine when escalation should occur, based on the classification of the request or incident.
2. Record all reported calls, incidents, service requests and information needs in an automated tool. Capture information including, but not limited to, type (e.g., hardware, software), status (e.g., new, assigned, escalated, closed) and the incident/problem owner.
3. Implement event detection mechanisms within systems monitoring tools for automated incident logging and alerting.
4. Record details of closed queries in the organisation's service management system in support of other processes, such as problem management, service level management, availability and capacity management.
5. Update the record status with all activities relating to the progress of the event. Enable involved parties to access relevant information in the service management system.
6. Use the service management system to report appropriate statistics and trends to senior management.

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

Control Practices

1. Ensure that the service desk maintains ownership, monitoring and escalation of requests and incidents on behalf of customers.
2. Notify management when high-impact incidents occur, e.g., major business impact or major deviation from agreed-upon service levels.
3. Define and implement a process to ensure that the incident records are updated to show the date, time and assignment to IT personnel.
4. Define and implement a process to ensure that IT staff members dealing with customer queries update the request or incident records with relevant information, such as classification, diagnosis, root cause and workarounds.

DS8 Manage Service Desk and Incidents (cont.)

Control Objective	Value Drivers	Risk Drivers
DS8.4 Incident Closure Establish procedures for the timely monitoring of clearance of customer queries. When the incident has been resolved, ensure that the service desk records the resolution steps, and confirm that the action taken has been agreed to by the customer. Also record and report unresolved incidents (known errors and workarounds) to provide information for proper problem management.	• 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

Control Practices

1. Define a process to manage the resolution and closure of each incident, including use of predetermined categorisations to identify the likely root cause of the incident.
2. Record all resolved incidents in detail and review the information for possible update in the knowledge base. Note the workaround and probable root cause for similar incidents arising in the future.
3. Monitor all request and incident records through the complete life cycle, and review them on a regular basis to guarantee timely resolution and fulfilment of customer queries.
4. Close requests and incidents only after confirmation of the initiator.

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

Control Practices

1. Define a process to identify, investigate and report on all queries in which the agreed-upon time frames for resolution (e.g., SLAs) were exceeded.
2. In support of problem identification, perform trend analysis on all queries to identify repeating incidents and patterns. Communicate to problem management for further actions.
3. Perform analysis of the feedback received from customers to evaluate trends related to the levels of satisfaction with the service provided by the service desk.
4. Compare service desk performance to industry standards. Take these results into account for continuous improvement.

DS9 Manage the Configuration

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

Control Practices

1. Implement a configuration repository to capture and maintain configuration management items. The repository should include hardware; application software; middleware; parameters; documentation; procedures; and tools for operating, accessing and using the systems, services, version numbers and licencing details.
2. Implement a tool to enable the effective logging of configuration management information within a repository.
3. Provide a unique identifier to a configuration item so the item can be easily tracked and related to physical asset tags and financial records.
4. Define and document configuration baselines for components across development, test and production environments, to enable identification of system configuration at specific points in time (past, present and planned).
5. Establish a process to revert to the baseline configuration in the event of problems, if determined appropriate after initial investigation.
6. Install mechanisms to monitor changes against the defined repository and baseline. Provide management reports for exceptions, reconciliation and decision making.

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

Control Practices

1. Define and implement a policy requiring all configuration items and their attributes and versions to be identified and maintained.
2. Tag physical assets according to a defined policy. Consider using an automated mechanism, such as barcodes.
3. Define a policy that integrates incident, change and problem management procedures with the maintenance of the configuration repository.
4. Define a process to record new, modified and deleted configuration items and their relative attributes and versions. Identify and maintain the relationships between configuration items in the configuration repository.
5. Establish a process to maintain an audit trail for all changes to configuration items.
6. Define a process to identify critical configuration items in relationship to business functions (component failure impact analysis).
7. Record all assets—including new hardware and software, procured or internally developed—within the configuration management data repository.
8. Define and implement a process to ensure that valid licences are in place to prevent the inclusion of unauthorised software.

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

Control Practices

1. To validate the integrity of configuration data, implement a process to ensure that configuration items are monitored. Compare recorded data against actual physical existence, and ensure that errors and deviations are reported and corrected.
2. Using automated discovery tools where appropriate, reconcile actual installed software and hardware periodically against the configuration database, licence records and physical tags.
3. Periodically review against the policy for software usage the existence of any software in violation or in excess of current policies and licence agreements. Report deviations for correction.

DS10 Manage Problems

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

Control Practices

1. Identify problems through the correlation of incident reports, error logs and other problem identification resources. Determine priority levels and categorisation to address problems in a timely manner.
2. Define and implement a problem-handling process that has access to all relevant data, including information from the change management system and IT configuration/asset and incident details, to effectively address the root cause(s).
3. Define appropriate support groups to assist with problem identification, root cause analysis and solution determination to support problem management. Determine support groups based on predefined categories, such as hardware, network, software, applications and support software.
4. Define priority levels through consultation with the business to ensure that problem identification and root cause analysis are handled in a timely manner according to the agreed-upon SLAs. Base priority levels on business impact and urgency.
5. Report the status of identified problems to the service desk so customers and IT management can be kept informed.

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

Control Practices

1. Establish and maintain a single problem management system to register and report problems identified and to establish audit trails of the problem management processes, including the status of each problem, i.e., open, reopen, in progress or closed. The system should register one record for each problem, including the needed information to understand the problem, relevant documentation of the problem, contact persons, time the problem was identified, known consequences, actual problem owner, any workaround performed, how and when solutions were implemented, and identification of the root cause.
2. Identify and implement a process for problems to be assigned and analysed in a timely manner to determine the root cause. Identify problems by comparing incident data with the database of known and suspected errors (e.g., those communicated by external vendors). Upon successful root cause identification, classify problems as known errors.
3. Associate the affected configuration items to the established/known error.
4. Produce reports to communicate the progress in resolving problems and to monitor the continuing impact of problems not solved. Monitor the status of the problem-handling process throughout its life cycle, including input from change and configuration management.
5. Produce reports to monitor the problem resolution against the business and customer SLAs. Ensure the proper escalation of problems, e.g., escalation to higher management level according to agreed-upon criteria, contacting external vendors or referring to the change advisory board to increase the priority of an urgent RFC to implement a temporary workaround.
6. To maximise resources and reduce turnaround, define and implement problem management procedures for the tracking of problem trends.
7. Identify and initiate sustainable solutions (permanent fix) addressing the root cause, and raise change requests via the established change management processes.

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

Control Practices

1. Define and implement a process 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.
2. Inform the service desk so users and customers can be informed of the schedule of problem closure, e.g., the schedule for fixing the known errors, the possible workaround or the fact that the problem will remain until the change is implemented, and the consequences of the approach taken.

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

Control Practices

1. Develop and implement a process to capture problem information related to IT changes and communicate it to key stakeholders. This communication could take the form of reports to and periodic meetings amongst problem, change and configuration management process owners to consider recent problems and potential corrective actions.
2. Ensure that process owners and managers from problem, change and configuration management meet regularly to discuss future planned changes.
3. To enable the organisation to monitor the total costs of problems, develop and implement a process to capture change efforts resulting from problem management process activities (e.g., fixes to problems and known errors) and report on them.
4. To determine the overall improvement of availability of IT services, monitor changes resulting from the problem management process. Monitor how the results of the problem management process decrease repeat incidents and reactive support requirements.

DS11 Manage 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 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

Control Practices

1. Define the business requirements for the management of data by IT.
2. Define and implement a policy that addresses segregation of duties within operations for the entry, processing and authorisation of data transactions, including overrides and corrections. Address the responsibilities for segregation of duties within both the business and operations.
3. Ensure that data completeness and restart and reprocessing requirements are included in batch job schedules and procedures.
4. Define and implement a process that ensures that data inputs are prepared with embedded checks for completeness, validity, accuracy, security, authorisation and integrity.
5. Define and implement a process that ensures that all operational errors requiring transaction reprocessing are brought to the attention of the originating business function and resubmitted in a timely fashion. All erroneous transactions should go through the same checks for segregation of duties, completeness, validity, etc., as for first-time data processing.
6. As appropriate and in accordance with defined security policies, communicate to management security breaches during any operational phase of data receipt, processing and transmission.
7. Define and implement a process that verifies and logs the distribution of the output to appropriate departments, with special handling of confidential information.
8. Define and implement a process that properly safeguards and stores source data and prevents their unauthorised modification.
9. Institute policies and procedures for retention of data received from the business and their subsequent destruction according to the data's sensitivity.

DS11 Manage Data (cont.)

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

Control Practices

1. Establish storage and retention procedures that address the organisation's security policy and change management procedures, including encryption and authentication. Consider the data and the keys and certificates used for encryption and authentication.
2. Establish storage and retention arrangements to satisfy legal, regulatory and business requirements for documents, data, archives, programmes, reports and messages (incoming and outgoing).
3. Define and implement procedures that describe the use of data management tools, e.g., control access, movement and purging of data.
4. Consider the impact of current and future changes in hardware and software standards on retrieval and processing of archived data.
5. Define and implement procedures that describe access to the data management tools and associated storage media. Restrict the access to authorised personnel.
6. Analyse media types of stored and archived data to define environmental requirements, e.g., humidity and temperature. Monitor and review the physical storage environment.
7. Periodically review the integrity and usability of magnetic media. Periodically report and track disk errors. Investigate trends to ensure that media can still be used. Replace media susceptible to degradation, such as tape and DVD-ROMs.

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

Control Practices

1. Assign responsibilities within the IT function for the development and maintenance of policies and procedures for media library management.
2. Ensure that the media library management system specifies security and access rights.
3. Maintain an inventory list of archived media to limit the opportunity for data loss.
4. Review on a regular basis the media inventoried against the list. Investigate and correct any discrepancies and missing media, and report to management.

DS11 Manage Data (cont.)

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

Control Practices

1. Clearly define responsibility for the development and communication of policies on disposal.
2. Sanitise equipment and media containing sensitive information prior to reuse or disposal. Such processes should ensure that data marked as ‘deleted’ or ‘to be disposed’ cannot be retrieved (e.g., media containing highly sensitive data should be physically destroyed).
3. To maintain an audit trail, log the disposal of equipment or media containing sensitive information.
4. Define a procedure to remove active media from the media inventory list upon disposal.
5. Transport unsanitised equipment and media in a secure way throughout the disposal process.
6. Require disposal contractors to 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

Control Practices

1. Periodically identify critical data that affect business operations, in alignment with the risk management model and IT service as well as the business continuity plan.
2. Define policies and procedures for the backup of systems, applications, data and documentation that 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
3. Assign responsibilities for taking and monitoring backups.
4. Schedule, take and log backups in accordance with established policies and procedures.
5. Ensure that systems, applications, data and documentation maintained or processed by third parties are adequately backed up or otherwise secured. Consider requiring return of backups from third parties. Consider escrow or deposit arrangements.
6. Define requirements for onsite and offsite storage of backup data that meet the business requirements. Consider the accessibility required to back up data.
7. Periodically perform sufficient restoration tests to ensure that all components of backups can be effectively restored.
8. Agree on and communicate with the business or IT process owner the time frame required for restoration.
9. Prioritise data recovery 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

Control Practices

1. Define and implement a process to clearly identify sensitive data. Consider the business need for confidentiality of the data, and applicable laws and regulations. Communicate and agree upon the classification of data with the business process owners.
2. Define and implement a policy 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.
3. Establish requirements for physical and logical access to data output. Clearly define and consider confidentiality of output.
4. Establish rules and procedures for end-user access to data and management and backup of sensitive data. Establish rules and procedures 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).
5. Ensure that appropriate programmes are instituted to create and maintain awareness of security in the handling and processing of sensitive data.
6. Ensure that sensitive information processing facilities are within secure physical locations. These should be protected by defined security perimeters coupled with appropriate surveillance, security barriers and entry controls. Consider the design of the physical infrastructure to prevent losses from fire, interference or external attack, or unauthorised access. Consider secure output drop-off points for sensitive outputs or transfer of data to third parties.

DS12 Manage the Physical Environment

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

Control Practices

1. Using the technology strategy, select a site for IT equipment that meets business requirements and the security policy. Take into account special considerations such as geographic position, neighbours and infrastructure. Other risks that need consideration include, but are not limited to, theft, air, fire, smoke, water, vibration, terror, vandalism, chemicals or explosives.
2. Define a process 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.
3. Ensure that the selection and design of the site take into account relevant laws and regulations, such as building codes and 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

Control Practices

1. Define and implement a policy for the physical security and access control measures to be followed for IT sites. Regularly review the policy to ensure that it remains relevant and up to date.
2. Limit the access to information about sensitive IT sites and the design plans. Ensure that external signs and other identification of sensitive IT sites are discreet and do not obviously identify the site from outside. Confirm that organisational directories/site maps do not identify the location of the IT site.
3. Design physical security measures to take into account the risk associated with the business and operation. Physical security measures include alarm systems, building hardening, armoured cabling protection and secure partitioning.
4. Periodically test and document the preventive, detective and corrective physical security measures to verify design, implementation and effectiveness.
5. Ensure that the site design takes into account the physical cabling of telecommunication and the piping of water, power and sewer. The installation must be concealed, so it is not directly visible. The piping of water and sewer must also be redirected away from the server rooms.
6. Define a process for the secure removal of IT equipment, supported by the appropriate authorisation.
7. Safeguard receiving and shipping areas of IT equipment in the same manner and scope as normal IT sites and IT operations.
8. Define and implement a policy and process to transport and store equipment securely.
9. Define a process to ensure that storage devices containing sensitive information are physically destroyed or sanitised.
10. Define a process for recording, monitoring, managing, reporting and resolving physical security incidents, in line with the overall IT incident management process.
11. Ensure that particularly sensitive sites are checked frequently (including weekends and holidays).

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

Control Practices

1. Define and implement a process that governs the requesting and granting of access to the computing facilities. Formal access requests are to be completed and authorised by management of the IT site, and the request records retained. The forms should specifically identify the areas to which the individual is granted access.
2. Define and implement procedures to ensure that access profiles remain current. Base access to IT sites (server rooms, buildings, areas or zones) on job function and responsibilities.
3. Define a process to log and monitor all entry points to IT sites. Register all visitors, including contractors and vendors, to the site.
4. Define and implement a policy instructing all personnel to display visible identification at all times. Prevent the issuance of identity cards or badges without proper authorisation.
5. Define and implement a policy requiring visitors to be escorted at all times while onsite by a member of the IT operations group. If a member of the group identifies an unaccompanied, unfamiliar individual who is not wearing staff identification, security personnel should be alerted.
6. Restrict access to sensitive IT sites by establishing perimeter restrictions, such as fences, walls, and security devices on interior and exterior doors. The devices record entry and sound an alarm in the event of unauthorised access. Examples of such devices include badges or key cards, keypads, closed-circuit television and biometric scanners.
7. Define a process to conduct regular physical security awareness training.

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

Control Practices

1. Establish and maintain a process to identify natural and man-made disasters that might occur in the area within which the IT facilities are located. Assess the potential effect on the IT facilities.
2. Define and implement a policy that identifies how IT equipment, including mobile and offsite equipment, is protected against environmental threats. The policy should limit or exclude eating, drinking and smoking in sensitive areas, and prohibit storage of stationery and other supplies posing a fire hazard within computer rooms.
3. Situate and construct IT facilities to minimise and mitigate susceptibility to environmental threats.
4. Define and implement a process to regularly monitor and maintain devices that proactively detect environmental threats (e.g., fire, water, smoke, humidity).
5. Define and implement procedures to respond to environmental alarms and other notifications. Document and test procedures, which should include prioritisation of alarms and contact with local emergency response authorities, and train personnel in these procedures.
6. Compare measures and contingency plans against insurance policy requirements, and report results. Address points of non-compliance in a timely manner.
7. Ensure that IT sites are built and designed to minimise the impact of environmental risks (e.g., theft, air, fire, smoke, water, vibration, terror, vandalism, chemicals, explosives). Consider specific security zones and/or fireproof cells (e.g., locating production and development environments/servers away from each other).
8. Keep the IT sites and server rooms clean and in a safe condition at all time, i.e., no mess, no paper or cardboard boxes, no filled dustbins, no flammable chemicals or materials.

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

Control Practices

1. Define and implement a process to examine the IT facilities' requirement for protection against environmental conditions, power fluctuations and outages, in conjunction with other business continuity planning requirements. Procure suitable uninterruptible supply equipment (e.g., batteries, generators) to support business continuity planning.
2. Regularly test the uninterruptible power supply's mechanisms and ensure that power can be switched to the supply without any significant effect on business operations.
3. Ensure that the facilities housing the IT systems have more than one source for dependent utilities (e.g., power, telecommunications, water, gas). Separate the physical entrance of each utility.
4. Confirm that cabling external to the IT site is located underground or has suitable alternative protection. Determine that cabling within the IT site is contained within secured conduits, and wiring cabinets have access restricted to authorised personnel. Properly protect cabling against damage caused by fire, smoke, water, interception and interference.
5. Ensure that cabling and physical patching (data and phone) are structured and organised. Cabling and conduit structures should be documented, e.g., blueprint building plan and wiring diagrams.
6. Analyse the facilities housing high-availability systems for redundancy and fail-over cabling requirements (external and internal).
7. Define and implement a process that ensures that IT sites and facilities are in ongoing compliance with relevant health and safety laws, regulations, guidelines, and vendor specifications.
8. Educate personnel on a regular basis on health and safety laws, regulations, and relevant guidelines. Educate personnel on fire and rescue drills to ensure knowledge and actions taken in case of fire or similar incidents.
9. Define and implement a process to record, monitor, manage and resolve facilities incidents in line with the IT incident management process. Make available reports on facilities incidents where disclosure is required in terms of laws and regulations.
10. Define a process to ensure that IT sites and equipment are maintained as per the supplier's recommended service intervals and specifications. The maintenance must be carried out only by authorised personnel.
11. Analyse physical alterations to IT sites or premises to reassess the environmental risk (e.g., fire or water damage). Report results of this analysis to business continuity and facilities management.

DS13 Manage Operations

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 quickly deal with operational problems, new staff and operational changes

Control Practices

1. Develop, implement and maintain standard IT operational procedures covering the definition of roles and responsibilities, including those of external service providers.
2. Train support personnel in operational procedures and related tasks for which they are responsible.
3. Define procedures and responsibilities for formal handover of duties (e.g., for shift change, planned or unplanned absence).
4. Define procedures for exception handling in line with the incident management and change management procedures and to address security aspects.
5. Ensure that segregation of duties is in line with the associated risk, security and audit requirements.

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

Control Practices

1. Use formal change control procedures for planning and scheduling processing activities. Gain authorisation for the initial schedules and changes to these schedules.
2. Ensure that the scheduling of batch jobs takes into consideration business requirements, priorities, conflicts between jobs and workload balancing. Put procedures in place to identify, investigate and approve departures from standard job schedules.
3. Define and implement a procedure to resolve and correct job failures.
4. Implement automated tools and processes to immediately notify and rectify critical processing failures.

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 incidents occur • Infrastructure problems causing greater operational and business impact than if they had been prevented or detected earlier • Poorly utilised and deployed infrastructure resources

Control Practices

1. Define and implement a process for event logging that identifies the level of information to be recorded based on a consideration of risk and performance.
2. Identify and maintain a list of infrastructure assets that need to be monitored based on service criticality, and the relationship between configuration items and services that depend on them.
3. Define and implement rules that identify and record threshold breaches and event conditions. Find a balance between generating spurious minor events and significant events so event logs are not overloaded with unnecessary information.
4. Produce event logs and retain them for an appropriate period to assist in future investigations.
5. Establish procedures for monitoring event logs and conduct regular reviews.
6. Ensure that incident tickets are created in a timely manner when monitoring activities identify deviations.

DS13 Manage Operations (cont.)

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

Control Practices

1. Establish procedures to govern the receipt, use, removal and disposal of special forms and output devices into, within and out of the organisation.
2. Assign access privileges to sensitive documents and output devices based on the least privilege principle, balancing risk and business requirements.
3. Establish an inventory of sensitive documents and output devices, and conduct regular reconciliations.
4. Establish appropriate physical safeguards over special forms and sensitive devices.
5. Define and implement a process for destroying sensitive information and output devices (e.g., degaussing of electronic media, physical destruction of memory devices, making shredders or locked paper baskets available to destroy special forms and other confidential papers).

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

Control Practices

1. Establish a preventive maintenance plan for all hardware, considering cost-benefit analysis, vendor recommendations, risk of outage, qualified personnel and other relevant factors.
2. Review all activity logs on a regular basis to identify critical hardware components that require preventive maintenance, and update the maintenance plan accordingly.
3. Establish maintenance agreements involving third-party access to organisational IT facilities for onsite and offsite activities (e.g., outsourcing). Establish formal service contracts containing or referring to all necessary security conditions, including access authorisation procedures, to ensure compliance with the organisational security policies and standards.
4. In a timely manner, communicate to affected customers and users the expected impact (e.g., performance restrictions) of maintenance activities.
5. Ensure that ports, services, user profiles or other means used for maintenance or diagnosis are active only when required.
6. Incorporate planned downtime in an overall production schedule, and schedule the maintenance activities to minimise the adverse impact on business processes.

ME—Monitor and Evaluate

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

CONTROL PRACTICES

ME1 Monitor and Evaluate IT Performance

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

Control Practices

1. Identify the relevant IT processes that support mission-critical business processes, strategic initiatives and the portfolio of IT-enabled investments. Categorise these IT processes in terms of impact to the business.
2. Define a monitoring approach that uses metrics based on IT's performance and that, when monitored, will indicate IT-driven business outcomes for the enterprise.
3. Establish and maintain an IT monitoring system that is tied to business strategies and facilitates effective monitoring of IT's support of business objectives. Integrate the IT monitoring approach within the enterprise's performance management approach.
4. Identify relationships and dependencies amongst the IT processes (e.g., expectation gaps, undefined interfaces, omissions, duplication of effort, inefficiencies) when monitoring IT performance.
5. Ensure that performance metrics cover:
   - Business contribution including, but not limited to, financials
   - Performance against the strategic business and IT plan
   - Risk and compliance with regulations
   - Internal and external user satisfaction with service levels
   - Key IT processes, including solution and service delivery
   - Future-oriented activities, e.g., emerging technology, reusable infrastructure, business and IT personnel skill sets

   Set performance metrics so they:
   - Represent IT's goals and objectives
   - Are based on accepted good practices
   - Focus on the most important practices
   - Are useful for internal and external comparison
   - Can be measured in terms of business impact
   - Are meaningful to IT's customers and sponsors
6. Agree with enterprise management on the key performance metrics that need to be reported. Agree on the key performance metrics with business management so the metrics are meaningful to the business. Obtain IT and business management approval of how IT's performance will be measured, and communicate the approach to all process stakeholders. Get process owners' commitment to regularly report on process performance in terms of the defined metrics.
7. Conduct regular reviews of the performance measurement approach, and revise or update the approach in accordance with management feedback or changing business needs.

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

Control Practices

1. Define targets 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.
2. Collect performance data needed by the monitoring approach in an automated fashion wherever feasible. Compare the measured performance to the targets at agreed-to intervals.
3. Ensure consistency, completeness and integrity of performance monitoring source data. Ensure control over all changes to performance monitoring data sources.
4. Define performance targets and focus on those that provide the largest insight-to-effort ratio.
5. Assess the integrity of the data collected 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

Control Practices

1. Select and deploy a monitoring and reporting system that is effective in recording and reporting the key performance metrics, provides for efficient data collection and reporting, and is integrated in the enterprise monitoring system.
2. Verify the quality and completeness of output in relation to agreed-upon measures.
3. Populate the performance measurement system with the targets and measurement data, preferably by using interfaces with automated data capturing. Verify the quality and completeness of input in relation to agreed-upon measures.
4. Design requirements for the IT process performance reports for integration into the IT monitoring system with data that are concise, easy to understand, and tailored to various management needs and audiences, including governance. Design reports to facilitate effective, timely decision making (e.g., scorecards, traffic light reports).
5. Design requirements for the IT performance reports so that IT's objectives (IT goals, IT process goals, IT activity goals), outcome and performance measures, and their cause-and-effect relationships are communicated in an understandable manner.

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

Control Practices

1. Compare the performance values to internal targets and benchmarks and, where possible, to external benchmarks (industry and key competitors).
2. Consider implementing in parallel with the performance management system a less formal feedback mechanism to obtain alternative measures of perceived performance. Use the data to improve the performance measurement system and, where necessary, solution and service delivery.
3. Assess performance against targets and analyse results. Compare measured performance to targets at agreed-to intervals. Ensure that performance targets and results are communicated to IT and senior and business management via the established performance monitoring framework.
4. Analyse the cause of deviations against targets, initiate remedial actions, assign responsibilities for remediation, and follow up. At appropriate times, review all deviations and search for root causes, where necessary. Document the issues for further guidance if the problem recurs. Collect and retain the appropriate evidence and documentation to support the analysis.
5. Where feasible, link achievement of performance targets to the organisational reward compensation system.

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

Control Practices

1. Establish a board and executive reporting process, based on the performance monitoring framework, for regular, accurate and timely reporting on IT's contribution to the business by measuring achievement of IT goals, mitigation of IT risks and the usage of resources.
2. Design senior management reports to 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.
3. Consolidate results of IT performance measurement. Translate them into business performance impacts (positive or negative) and incorporate the results into standard periodic reports to the board. Clearly link IT performance measurement to business outcomes and identify how IT supports business strategy.

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 fashion • 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

Control Practices

1. Design processes, policies and procedures to initiate, prioritise and allocate responsibility for remedial actions to improve IT's solution and service delivery capability and performance. Ensure that appropriate tracking of actions is taken.
2. Initiate remedial action tasks based on the agreed-upon processes, policies and procedures. Define clear outcomes and conduct periodic progress reviews.
3. Identify specific significant deviations in corrective action implementation and generally substandard performance trends, and escalate those to senior management.
4. Upon satisfactory completion, compare remedial action tasks against prespecified outcomes and recognise good performance in process improvement. Follow up on the completion of remedial actions and learn from experiences to avoid future deviations.
5. Provide training to ensure that the organisation has adequate skills in measurement, data collection and analysis, and that staff members adopt and promote the performance measurement culture.

ME2 Monitor and Evaluate Internal Control

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

Control Practices

1. Define and implement a policy based on organisational governance standards and industry-accepted frameworks and practices, with associated ongoing internal control monitoring and evaluation activities. Consider organisational governance standards for internal control and risk management.
2. Consider independent evaluations of the IT internal control system (e.g., by internal audit or peers).
3. Identify the boundaries of the IT internal control system (e.g., consider how organisational IT internal controls take into account outsourced development or production activities).
4. Establish processes or procedures to ensure that control activities are in place and exceptions are promptly reported, followed up and analysed. Ensure that appropriate corrective actions are chosen and implemented. Prioritise control exceptions according to the risk management profile (e.g., classify certain exceptions as key risks and others as non-key risks).
5. Maintain the IT internal control system, considering ongoing changes in the organisational control environment, relevant business processes and IT risks. If gaps exist, evaluate and recommend changes.
6. Regularly evaluate the performance of the IT control framework, comparing performance indicators against industry accepted standards and good practices. Consider formal adoption of a continuous improvement approach to internal control monitoring.

ME2 Monitor and Evaluate Internal Control (cont.)

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

Control Practices

1. Identify and review internal controls that require managerial oversight, considering the criticality and risk of IT process activities. Consider corporate and IT policies on risk management, information security, privacy, and compliance with laws and regulations.
2. Ensure that managerial oversight and review of internal control are appropriately documented.
3. Define an escalation process for issues identified by managerial reviews. Ensure that the process considers the reasons for escalation and the level to which issues are to be escalated. Ensure that the process requires documentation of issues and resulting escalation.
4. Consider implementing automated control monitoring and reporting systems.
5. Ensure that managerial controls are established over the controls included in SLAs with the business and third parties.

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 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

Control Practices

1. Establish processes for identifying, reporting, logging and assigning responsibility for reporting and resolving control exceptions (e.g., security breaches, application program abends and network failures). Ensure that the processes address timely reporting and resolution.
2. Considering related business risks, establish policies and standards to establish thresholds for escalation of control exceptions and breakdowns.
3. Communicate procedures for escalation and root cause analysis and reporting same to business process owners and IT stakeholders.
4. Decide which control exceptions should be communicated to the individual responsible for the function and which exceptions should be escalated. Inform affected business process owners and IT stakeholders.
5. Assign accountability for root cause analysis and reporting.

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

Control Practices

1. Define a plan and scope, and identify evaluation criteria for conducting self-assessments. Plan the communication of results of the self-assessment process to IT and general management and the board. Consider internal audit standards in the design of self-assessments.
2. Determine the frequency of periodic self-assessments, taking into account the effectiveness of ongoing monitoring.
3. Assign responsibility for self-assessment to appropriate individuals to ensure objectivity and competence.
4. Provide for independent reviews to ensure objectivity of the self-assessment and enable the sharing of internal control good practices.
5. Compare the results of the self-assessments against industry standards and good practices.
6. Summarise and report outcomes of self-assessments and benchmarking for remedial actions.

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

Control Practices

1. Obtain independent control reviews (e.g., by an internal or external auditor or specialist IT governance consultant), certifications or accreditations. Consider the frequency of reviews in line with the risk profile and business objectives.
2. Ensure that staff members or external specialists are independent and competent to perform reviews, certifications or accreditations (e.g., reviewers hold Certified Information Systems Auditor™ [CISA®] certification).
3. Confirm that contractual conditions ensure that an adequate scope is performed, liability is established for incorrect opinions and confidentiality is maintained. If a formal certificate is to be obtained, obtain it from an organisation that is an accredited certification authority.
4. Report any significant internal control deficiencies identified for business process owner and IT management attention. Ensure that deficiencies are reported in a manner appropriate for the audience.

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

Control Practices

1. Ensure that appropriate internal control requirements are addressed in third-party contract agreements. Where appropriate, ensure that the contract has provisions for audit or review, e.g., certification/accreditation review, an appropriate audit engagement (e.g., SAS 70 Type II engagement), or by direct audit of the service provider by IT management.
2. Ensure that third-party service providers comply with applicable laws, regulations and contractual commitments. Communicate to business process owners, IT management and third-party service providers any failure to comply with such commitments.
3. Confirm receipt of any required legal or regulatory internal control assertions from affected third-party service providers. Investigate exceptions. Obtain assertions from the service provider that appropriate remedial actions will be completed according to an agreed-upon remediation plan.

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

Control Practices

1. Assess control exceptions. Decide which control exceptions must be remediated, in line with the business needs, risk profile and regulatory and compliance requirements. Involve business process owners in the assessment process, where appropriate. Communicate outcomes of the assessment process to the board, senior management, business process owners and IT stakeholders, as appropriate.
2. Design an approach to prioritise and assign responsibility for all control remedial actions.
3. Initiate remedial action tasks based on the agreed-upon approach. Ensure proper tracking and reporting of the status of remedial action tasks.
4. Identify substandard performance in internal control and/or in correcting internal control weaknesses, and specify corrective actions.
5. Escalate continued substandard performance in internal control and/or in correcting internal control weaknesses to business process owners and IT senior management for further action, where appropriate.
6. Approve remedial action tasks upon satisfactory completion against prespecified outcomes.

ME3 Ensure Compliance With External Requirements

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

Control Practices

1. Assign responsibility for the identification of legal or regulatory requirements relevant to the IT resources and operations of the organisation. Consider contractual requirements between trading partners and with service providers with respect to security, privacy, data handling, intellectual property and copyright, and insurance contracts.
2. Design and implement a process to identify and assess the applicable laws and regulatory requirements. Determine their impact on the IT resources and operations of the organisation and its service providers, and update policies, standards, procedures and methodologies accordingly. Consider laws and regulations for electronic commerce, data flow, security, privacy, internal controls, financial reporting, industry-specific regulations, intellectual property copyright, and health and safety, and ensure that these obligations are included in the contractual terms.
3. Assess the impact of legal and regulatory requirements on contracts related to IT operations, contractual relationships, third-party service providers and trading partners.
4. Obtain independent counsel, where appropriate, on changes to applicable laws, regulations and standards.
5. Maintain an up-to-date log of all relevant legal, regulatory and contractual compliance requirements; their impact; and required actions.

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

Control Practices

1. Review and revise, as necessary, the policies, standards, procedures and methodologies to ensure compliance with legal and regulatory requirements.
2. Regularly review policies, standards, procedures and methodologies for their effectiveness in ensuring necessary compliance using internal and external experts.
3. Obtain expert independent advice, where appropriate, on policies, standards, procedures and methodologies content and implementation.
4. Communicate new and changed requirements to all relevant personnel.

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

Control Practices

1. Regularly evaluate IT organisational policies, standards, procedures and methodologies to ensure compliance with relevant legal, regulatory and contractual requirements. Ensure that gaps are addressed and changes are reflected in the policies, standards and procedures on a timely basis.
2. Periodically evaluate IT processes and activities to ensure adherence to applicable legal, regulatory and contractual requirements.
3. Regularly evaluate recurring patterns of compliance failures. Where necessary, improve policies, standards, procedures, methodologies, and associated processes and activities.

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

Control Practices

1. Obtain regular confirmation of compliance with internal policies from process owners.
2. Ensure that regular (and, where appropriate, independent) internal and external reviews are performed to assess levels of compliance with internal policies.
3. Establish procedures for the receipt of assertions from third-party service providers on levels of their compliance with applicable laws and regulations.
4. Ensure that contracts with third-party service providers require regular confirmation of their compliance with applicable laws and regulations.
5. Implement a process to monitor and report on non-compliance issues, with further investigation, where necessary, of the root cause of non-compliant performance 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

Control Practices

1. Co-ordinate requirements for corporate reporting on legal, regulatory and contractual compliance, including the requirement to retain historical information.
2. To ensure reporting consistency and completeness, ensure that IT compliance status reporting conforms with corporate reporting requirements, such as distribution, frequency, scope, content and format.

ME4 Provide IT Governance

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

Control Practices

1. Establish an IT strategy committee to provide high-level policy guidance (e.g., risk, funding, sourcing, partnering) and verify strategy compliance (e.g., achievement of strategic goals and objectives).
2. Establish processes to define IT enabled investment priorities, assess strategic fit of proposals and perform investment portfolio reviews for continuing strategic relevance.
3. Establish appropriate management structures such as an IT steering committee, technology council, IT architecture review board and IT audit committee.
4. Establish IT investment portfolio management disciplines, which include periodic review of portfolios to verify their continued relevance to the business.
5. Embed into the enterprise an IT governance structure and culture that is accountable, effective and transparent, with defined activities and purposes and with unambiguous responsibilities.
6. Aggregate all IT governance issues and remedial actions into a consolidated management context for reporting. Report to the board the status of IT governance issues and activities and identify their impact on strategic initiatives and enterprise outcomes.

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

Control Practices

1. Enable an effective enterprise strategic planning process by ensuring alignment between the business and IT strategy and an IT organizational structure that complements the business model and direction.
2. Align and integrate the IT strategy with business goals. Provide direction so that IT is optimally enabling the business strategy and that IT operations are aligned with business operations. There should be appropriate mediation between imperatives of the business and of the technology.
3. Direct designated business sponsors to be actively involved, accountable and owners of major IT-enabled investments.

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

Control Practices

1. Monitor delivery of IT services to ensure that they support and provide benefit to business processes. Direct IT investment programmes to ensure that they deliver tangible benefits in keeping with original objectives. Establish co-responsibility between the business and IT for IT investments.
2. Establish IT and business architectures that are designed to drive maximum business value. Standardise architectures and technology to reduce complexity and achieve cost optimisation.
3. Monitor whether IT investments are based on a balance of risk and benefit, with budgets that are acceptable and take into account return and competitive aspects of IT investments.
4. Evaluate the IT asset portfolio on a regular basis to ensure that value in relation to costs is optimised.
5. Monitor the IT budget and investment plan to ensure that they are realistic and integrated into the overall financial plan.
6. Proactively seek ways to ensure that IT initiatives are managed with a view to enhancing enterprise value whilst managing business and executive expectations.

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

Control Practices

1. Provide high-level direction for sourcing and use of IT resources, e.g., strategic alliances.
2. Monitor how management determines what IT resources are needed to achieve strategic goals. Establish business priorities and allocate resources to enable effective IT performance.
3. Optimise and balance overall IT investments and use of resources between sustaining and growing the enterprise.
4. Direct the organisation to be in the best position to capitalise on its information and knowledge resources.
5. Monitor the adequacy of the IT infrastructure to ensure that it facilitates creation and sharing of business information at optimal cost.
6. Monitor and ensure the availability of suitable IT resources, skills and infrastructure to meet the strategic objectives. Allocate and define roles critical for driving maximum value from IT, and ensure appropriate staffing and resources.

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

Control Practices

1. Provide the board with information on IT risk exposures and the measures in place dealing with risk containment and associated costs. Confirm the appropriateness of the risk management plan and its alignment with the appetite for risk.
2. Monitor risk management practices to ensure that risk management is operating as required, responsibilities for risk management are appropriately and unambiguously assigned, and management has resources in place to ensure proper management of IT risks.
3. Evaluate the effectiveness of management's monitoring of IT risks.
4. Review the outcome of management's evaluation of the risk of IT activities. Confirm that the total risk exposure does not exceed the defined risk appetite, considering mitigating controls in place. Oversee the implementation of additional mitigating controls to reduce the overall risk exposure as needed.

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

Control Practices

1. Assess senior management's performance in the execution and achievement of IT strategies and alignment with business strategies. Review significant failures and provide direction to rectify organisational or systemic causes through appropriate corrective actions.
2. Obtain assurance of the satisfactory performance and control and risk management of IT and that the major IT decisions have been made appropriately. Consider independent assurance (internal or external) where an objective or specialist's opinion is required.
3. Direct the IT scorecard to be properly linked to business goals and accepted by the business. Compare the measurement of IT performance with the contribution of IT to the business (i.e., delivering the promised business value).

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

Control Practices

1. Define and implement an organisational structure to obtain independent assurance. This typically includes an audit committee and supporting technical board-level committees, as appropriate, 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 on the completion of recommendations.
2. Obtain independent reviews and certifications of compliance with IT policies, standards and procedures using internal audit and/or external parties.
3. Consider the following advisor selection criteria in obtaining balanced assurance: independence, objectivity, confidentiality, integrity, proficiency and due professional care, and qualifications/certifications to perform the work.

AC — Application Control

CONTROL PRACTICES

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

Control Practices

1. Design source documents in a way that they increase accuracy with which data can be recorded, control the workflow and facilitate subsequent reference checking. Where appropriate, include completeness controls in the design of the source documents.
2. Create and document procedures for preparing source data entry, and ensure that they are effectively and properly communicated to appropriate and qualified personnel. These procedures should establish and communicate required authorisation levels (input, editing, authorising, accepting and rejecting source documents). The procedures should also identify the acceptable source media for each type of transaction.
3. Ensure that the function responsible for data entry maintains a list of authorised personnel, including their signatures.
4. Ensure that all source documents include standard components and contain proper documentation (e.g., timeliness, predetermined input codes, default values) and are authorised by management.
5. Automatically assign a unique and sequential identifier (e.g., index, date and time) to every transaction.
6. Return documents that are not properly authorised or are incomplete to the submitting originators for correction, and log the fact that they have been returned. Review logs periodically to verify that corrected documents are returned by originators in a timely fashion, and to enable pattern analysis and root cause review.

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

Control Practices

1. Define and communicate criteria for timeliness, completeness and accuracy of source documents. Establish mechanisms to ensure that data input is performed in accordance with the timeliness, accuracy and completeness criteria.
2. Use only prenumbered source documents for critical transactions. If proper sequence is a transaction requirement, identify and correct out-of-sequence source documents. If completeness is an application requirement, identify and account for missing source documents.
3. Define and communicate who can input, edit, authorise, accept and reject transactions, and override errors. Implement access controls and record supporting evidence to establish accountability in line with role and responsibility definitions.
4. Define procedures to correct errors, override errors and handle out-of-balance conditions, as well as to follow up, correct, approve and resubmit source documents and transactions in timely manner. These procedures should consider things such as error message descriptions, override mechanisms and escalation levels.
5. Generate error messages in a timely manner as close to the point of origin as possible. The transactions should not be processed unless errors are corrected or appropriately overridden or bypassed. Errors that cannot be corrected immediately should be logged in an automated suspense log, and valid transaction processing should continue. Error logs should be reviewed and acted upon within a specified and reasonable period of time.
6. Ensure that errors and out-of-balance reports are reviewed by appropriate personnel, followed up and corrected within a reasonable period of time, and that, where necessary, incidents are raised for more senior attention. Automated monitoring tools should be used to identify, monitor and manage errors.
7. Ensure that source documents are safe-stored (either by the business or by IT) for a sufficient period of time in line with legal, regulatory or business requirements.

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

Control Practices

1. Ensure that transaction data are verified as close to the data entry point as possible and interactively during online sessions. Ensure that transaction data, whether people-generated, system-generated or interfaced inputs, are subject to a variety of controls to check for accuracy, completeness and validity. Wherever possible, do not stop transaction validation after the first error is found. Provide understandable error messages immediately such that they enable efficient remediation.
2. Implement controls to ensure accuracy, completeness, validity and compliancy to regulatory requirements of data input. Controls may include 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), duplicate and logical relationship checks, and time edits. Validation criteria and parameters should be subject to periodic reviews and confirmation.
3. Establish access control and role and responsibility mechanisms so that only authorised persons input, modify and authorise data.
4. Define requirements for segregation of duties for entry, modification and authorisation of transaction data as well as for validation rules. Implement automated controls and role and responsibility requirements.
5. Report transactions failing validation and post them to a suspense file. Report all errors in a timely fashion, and do not delay processing of valid transactions.
6. Ensure that transactions failing edit and validation routines are subject to appropriate follow-up until errors are remediated. Ensure that information on processing failures is maintained to allow for root cause analysis and help adjust procedures and automated controls.

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

Control Practices

1. Establish and implement mechanisms to authorise the initiation of transaction processing and to enforce that only appropriate and authorised applications and tools are used.
2. Routinely verify that processing is completely and accurately performed with automated controls, where appropriate. Controls may include checking for sequence and duplication errors, transaction/record counts, referential integrity checks, control and hash totals, range checks, and buffer overflow.
3. Ensure that transactions failing validation routines are reported and posted to a suspense file. Where a file contains valid and invalid transactions, ensure that the processing of valid transactions is not delayed and that all errors are reported in a timely fashion. Ensure that information on processing failures is kept to allow for root cause analysis and help adjust procedures and automated controls, to ensure early detection or to prevent errors.
4. Ensure that transactions failing validation routines are subject to appropriate follow-up until errors are remediated or the transaction is cancelled.
5. Ensure that the correct sequence of jobs has been documented and communicated to IT operations. Job output should include sufficient information regarding subsequent jobs to ensure that data are not inappropriately added, changed or lost during processing.
6. Verify the unique and sequential identifier to every transaction (e.g., index, date and time).
7. Maintain the audit trail of transactions processed. Include date and time of input and user identification for each online or batch transaction. For sensitive data, the listing should contain before and after images and should be checked by the business owner for accuracy and authorisation of changes made.
8. Maintain the integrity of data during unexpected interruptions in data processing with system and database utilities. Ensure that controls are in place to confirm data integrity after processing failures or after use of system or database utilities to resolve operational problems. Any changes made should be reported and approved by the business owner before they are processed.
9. Ensure that adjustments, overrides and high-value transactions are reviewed promptly in detail for appropriateness by a supervisor who does not perform data entry.
10. Reconcile file totals. For example, a parallel control file that records transaction counts or monetary value as data should be processed and then compared to master file data once transactions are posted. Identify, report and act upon out-of-balance conditions.

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 occur; 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

Control Practices

1. When handling and retaining output from IT applications, follow defined procedures and consider privacy and security requirements. Define, communicate and follow procedures for the distribution of output.
2. At appropriate intervals, take a physical inventory of all sensitive output, such as negotiable instruments, and compare it with inventory records. Create procedures with audit trails to account for all exceptions and rejections of sensitive output documents.
3. Match control totals in the header and/or trailer records of the output to balance with the control totals produced by the system at data entry to ensure completeness and accuracy of processing. If out-of-balance control totals exist, report them to the appropriate level of management.
4. Validate completeness and accuracy of processing before other operations are performed. If electronic output is reused, ensure that validation has occurred prior to subsequent uses.
5. Define and implement procedures to ensure that the business owners review the final output for reasonableness, accuracy and completeness, and that output is handled in line with the applicable confidentiality classification. Report potential errors, log them in an automated, centralised logging facility, and address errors in a timely manner.
6. If the application produces sensitive output, define who can receive it, label the output so it is recognisable by people and machines, and implement distribution accordingly. Where necessary, send it to special access-controlled output devices.

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

Control Practices

1. Where transactions are exchanged electronically, establish an agreed-upon standard of communication and mechanisms necessary for mutual authentication, including how transactions will be represented, the responsibilities of both parties and how exception conditions will be handled.
2. Tag output from transaction processing applications in accordance with industry standards to facilitate counterparty authentication, provide evidence of non-repudiation, and allow for content integrity verification upon receipt by the downstream application.
3. Analyse input received from other transaction processing applications to determine authenticity of origin and the maintenance of the integrity of content during transmission.

Page intentionally left blank

Appendix

CobiT and Related Products

APPENDIX—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 good practice management objectives for IT processes
- Management guidelines—Offer tools to help assign responsibility, measure performance, and benchmark and address gaps in capability
- Maturity models—Provide profiles of IT processes describing possible current and future states

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

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

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

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

Page intentionally left blank