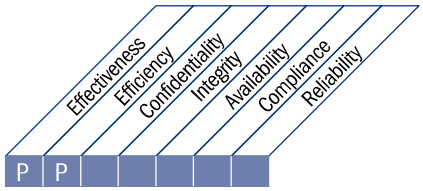
Process Description

PO4 Define the IT Processes, Organisation and Relationships

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



Control over the IT process of

Define the IT processes, organisation and relationships

that satisfies the business requirement for IT of

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

by focusing on

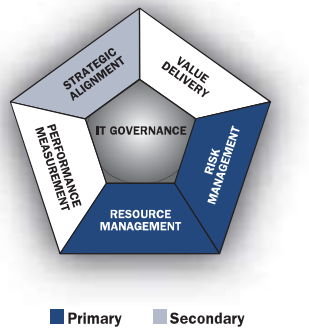
establishing transparent, flexible and responsive IT organisational structures and defining and implementing IT processes with owners, roles and responsibilities integrated into business and decision processes

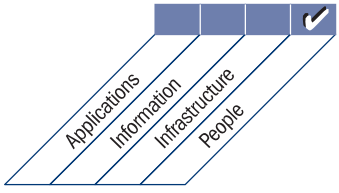
is achieved by

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

and is measured by

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





Control Objectives

PO4 Define the IT Processes, Organisation and Relationships

PO4.1 IT Process Framework
Define an IT process framework to execute the IT strategic plan. This framework should include an IT process structure and relationships (e.g., to manage process gaps and overlaps), ownership, maturity, performance measurement, improvement, compliance, quality targets and plans to achieve them. It should provide integration amongst the processes that are specific to IT, enterprise portfolio management, business processes and business change processes. The IT process framework should be integrated into a quality management system (QMS) and the internal control framework.

PO4.2 IT Strategy Committee
Establish an IT strategy committee at the board level. This committee should ensure that IT governance, as part of enterprise governance, is adequately addressed; advise on strategic direction; and review major investments on behalf of the full board.

PO4.3 IT Steering Committee
Establish an IT steering committee (or equivalent) composed of executive, business and IT management to:
- Determine prioritisation of IT-enabled investment programmes in line with the enterprise's business strategy and priorities
- Track status of projects and resolve resource conflict
- Monitor service levels and service improvements

PO4.4 Organisational Placement of the IT Function
Place the IT function in the overall organisational structure with a business model contingent on the importance of IT within the enterprise, specifically its criticality to business strategy and the level of operational dependence on IT. The reporting line of the CIO should be commensurate with the importance of IT within the enterprise.

PO4.5 IT Organisational Structure
Establish an internal and external IT organisational structure that reflects business needs. In addition, put a process in place for periodically reviewing the IT organisational structure to adjust staffing requirements and sourcing strategies to meet expected business objectives and changing circumstances.

PO4.6 Establishment of Roles and Responsibilities
Establish and communicate roles and responsibilities for IT personnel and end users that delineate between IT personnel and end-user authority, responsibilities and accountability for meeting the organisation's needs.

PO4.7 Responsibility for IT Quality Assurance
Assign responsibility for the performance of the quality assurance (QA) function and provide the QA group with appropriate QA systems, controls and communications expertise. Ensure that the organisational placement and the responsibilities and size of the QA group satisfy the requirements of the organisation.

PO4.8 Responsibility for Risk, Security and Compliance
Embed ownership and responsibility for IT-related risks within the business at an appropriate senior level. Define and assign roles critical for managing IT risks, including the specific responsibility for information security, physical security and compliance. Establish risk and security management responsibility at the enterprise level to deal with organisationwide issues. Additional security management responsibilities may need to be assigned at a system-specific level to deal with related security issues. Obtain direction from senior management on the appetite for IT risk and approval of any residual IT risks.

PO4.9 Data and System Ownership
Provide the business with procedures and tools, enabling it to address its responsibilities for ownership of data and information systems. Owners should make decisions about classifying information and systems and protecting them in line with this classification.

PO4.10 Supervision
Implement adequate supervisory practices in the IT function to ensure that roles and responsibilities are properly exercised, to assess whether all personnel have sufficient authority and resources to execute their roles and responsibilities, and to generally review KPIs.

PO4.11 Segregation of Duties
Implement a division of roles and responsibilities that reduces the possibility for a single individual to compromise a critical process. Make sure that personnel are performing only authorised duties relevant to their respective jobs and positions.

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

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

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

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

Page intentionally left blank

Management Guidelines

PO4 Define the IT Processes, Organisation and Relationships

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

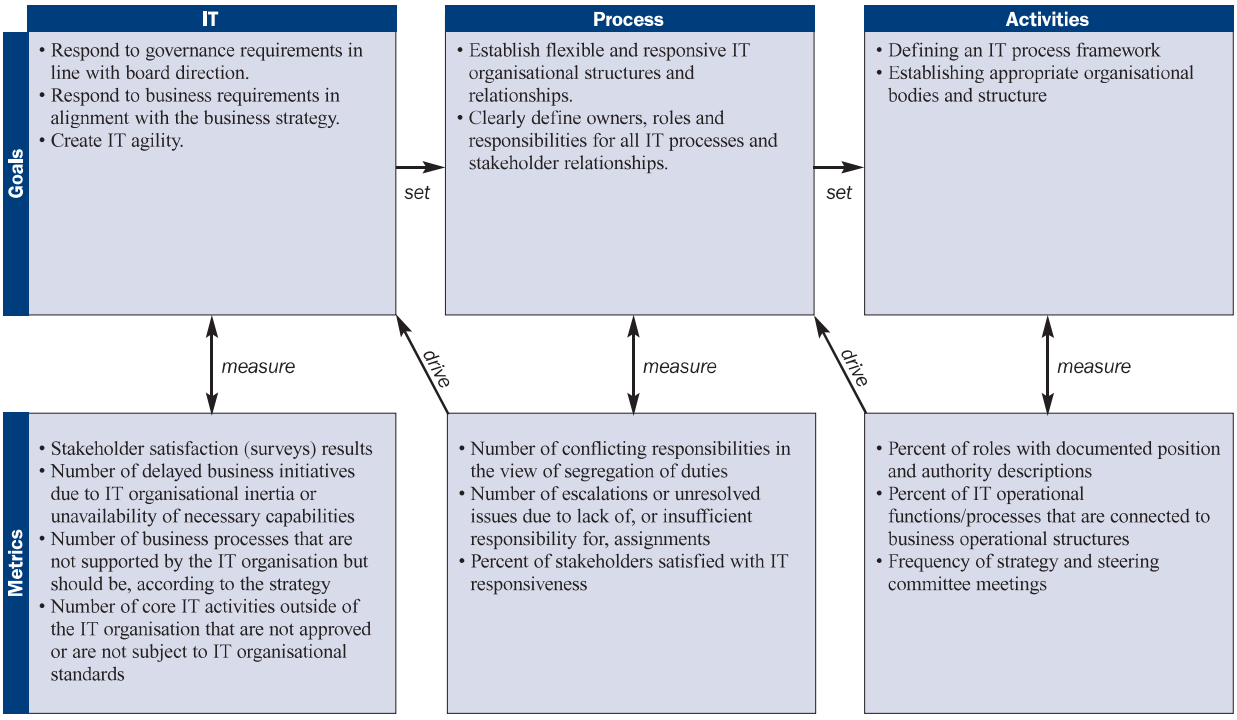
Outputs	To
IT process framework	ME4
Documented system owners	AI7, DS6
IT organisation and relationships	PO7
IT process framework, documented roles and responsibilities	ALL
Document roles and responsibilities	PO7

RACI Chart

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

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

Goals and Metrics



Maturity Model

PO4 Define the IT Processes, Organisation and Relationships

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

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

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

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

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

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

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