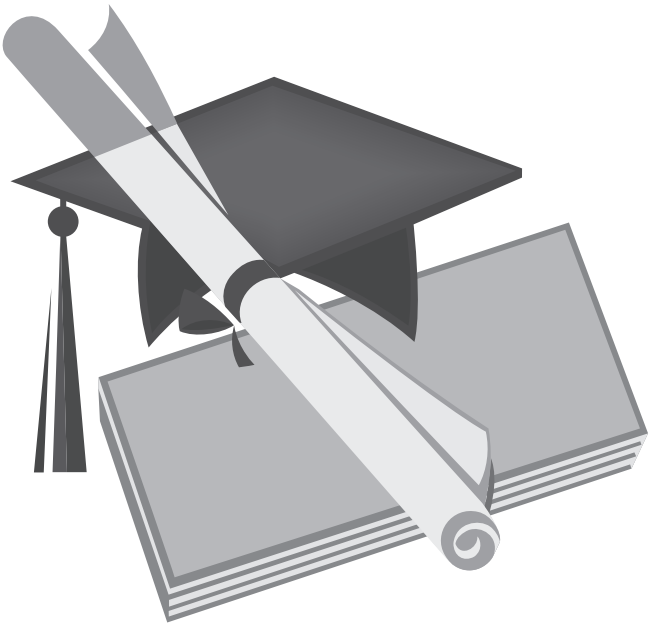
COBIT® STUDENT BOOK



Provides high-quality educational material on COBIT® and its implementations that can be integrated into curricula on information systems management, information security management, auditing, information systems auditing or accounting information systems

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. The IT Governance Institute offers symposia, original research and case studies to assist enterprise leaders and boards of directors in their IT governance responsibilities.

Information Systems Audit and Control Association®
With more than 35,000 members in more than 100 countries, the Information Systems Audit and Control Association (ISACA®) (*www.isaca.org*) is a recognised worldwide leader in IT governance, control, security and assurance. Founded in 1969, ISACA sponsors international conferences, publishes the *Information Systems Control Journal®*, develops international information systems auditing and control standards, and administers the globally respected Certified Information Systems Auditor™ (CISA®) designation, earned by more than 35,000 professionals since inception, and the Certified Information Security Manager® (CISM®) designation, a groundbreaking credential earned by 5,000 professionals in its first two years.

Disclaimer
The IT Governance Institute, Information Systems Audit and Control Association [the "Owner(s)"] and the authors have designed and created *COBIT in Academia* and its related publications, titled COBIT® *Caselets*, COBIT® *Student Book*, COBIT® *Case Study: TIBO* and COBIT® *Presentation Package*, (the "Work"), primarily as an educational resource for educators. The Owners make no claim that use of any of the Work will assure a successful outcome. The Work should not be considered inclusive of any proper information, procedures and tests or exclusive of other information, procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific information, procedure or test, the educator should apply his/her own professional judgement to the specific 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: *research@isaca.org*
Web sites: *www.itgi.org* and *www.isaca.org*

ISBN 1-893209-96-2
COBIT in Academia
Printed in the United States of America

ACKNOWLEDGEMENTS

IT GOVERNANCE INSTITUTE WISHES TO RECOGNISE:

The Board of Trustees
Marios Damianides, CISA, CISM, CA, CPA, Ernst & Young LLP, USA, International President
Abdul Hamid Bin Abdullah, CISA, CPA, Auditor General's Office, Singapore, Vice President
William C. Boni, CISM, Motorola, USA, Vice President
Ricardo Bria, CISA, SAFE Consulting Group, Spain, Vice President
Everett C. Johnson, CPA, Deloitte & Touche LLP (retired), USA, Vice President
Howard Nicholson, CISA, CRN Solutions, Australia, Vice President
Bent Poulsen, CISA, CISM, VP Securities Services, Denmark, Vice President
Frank K. M. Yam, CISA, CIA, CCP, CFE, Focus Strategic Group Inc., Hong Kong, Vice President
Robert S. Roussey, CPA, University of Southern California, USA, Past International President
Paul A. Williams, FCA, MBCS, Paul Williams Consulting, UK, Past International President
Emil D'Angelo, CISA, CISM, Bank of Tokyo-Mitsubishi, USA, Trustee
Ronald Saull, CSP, Great-West Life and IMG Financial, Canada, Trustee
Erik Guldentops, CISA, CISM, Belgium, Advisor, IT Governance Institute

The Development Team
Erik Guldentops, CISA, CISM, University of Antwerp Management School, Belgium (Chair)
Roger Debreceny, Ph.D., FCPA, University of Hawaii, USA
Steven De Haes, University of Antwerp Management School, Belgium (Project Manager)
Roger Lux, Farmers Insurance Group, USA
John Mitchell, CISA, CIA, CFE, LHS Business Control, UK
Ed O'Donnell, Ph.D., Arizona State University, USA
Scott Summers, Ph.D., Brigham Young University, USA
Wim Van Grembergen, Ph.D., University of Antwerp Management School, Belgium

The Review Team
Georges Ataya, CISA, CISM, CISSP, Solvay Business School, Belgium
Janie Chang, Ph.D., San Jose State University, USA
Frederick Gallegos, CISA, CGFM, CDE, California State Polytechnic University at Pomona, USA

TABLE OF CONTENTS

PURPOSE OF THIS DOCUMENT

The goal of the *Student Book* is to provide high-quality educational material on COBIT and its implementations that can be integrated into curricula for students in information systems management, information security management, auditing, information systems auditing or accounting information systems. It was developed by the IT Governance Institute, in collaboration with a group of international academics and practitioners.

The *Student Book* is composed of three parts. Chapter 1 explains all the aspects of the COBIT framework in detail. Chapter 2 takes this knowledge one level further by discussing in detail how the elements of the COBIT framework can be applied, specifically for managing third-party services (COBIT process DS2). Both chapters 1 and 2 provide numerous examples and testimonials that illustrate the COBIT framework and its use in practice. Chapter 3 provides the COBIT elements for eight of the 34 COBIT processes (as selected by the authors of this book): PO1, PO9, PO10, AI2, DS5, DS6, M1 and M2. The information in chapter 3 can be used by students as guidance while working on specific COBIT exercises.

The IT Governance Institute has also developed three other products that can accompany this COBIT *Student Book*: the COBIT Presentation Package, providing a comprehensive 80-slide PowerPoint deck explaining all the COBIT elements; the COBIT *Case Study: TIBO* (graduate level), which can be used by students to apply the COBIT knowledge in a real-life situation; and COBIT *Caselets*, which are some minicases for smaller exercises at the undergraduate level.

Chapter 1: The CobiT Framework

In recent years, it has become increasingly evident that there is a need for a reference framework for developing and managing internal controls and appropriate levels of security in information technology (IT). The application of IT has become central to the strategy and business processes of many entities. As such, successful organisations require an appreciation for and a basic understanding of the risks and constraints of IT at all levels within the enterprise in order to achieve effective direction and adequate controls. CobiT (*Control Objectives for Information and related Technology*) provides such a control and security framework for IT. The CobiT framework is explained in this chapter.

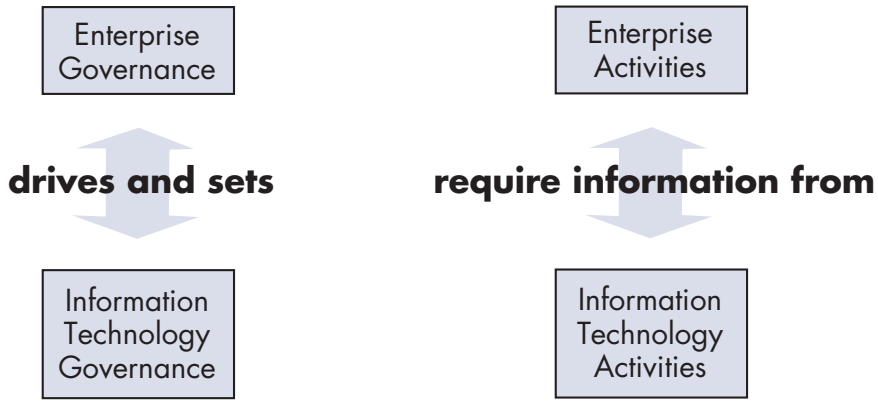
CobiT CONTEXT: EMERGENCE OF ENTERPRISE AND IT GOVERNANCE

Information technology is an important factor in achieving success in the information economy and central to an entity's operational and financial management. As a result, enterprise governance and IT governance can no longer be considered separate and distinct disciplines. Effective enterprise governance focuses individual and group expertise and experience where it can be most productive, monitors and measures performance, and provides assurance to critical issues. IT, long considered solely an enabler of an enterprise's strategy, must now be regarded as an integral part of that strategy.

IT governance provides the structure that links IT processes, IT resources and information to enterprise strategies and objectives. IT governance integrates and institutionalises optimal ways of planning and organising, acquiring and implementing, delivering and supporting, and monitoring and evaluating IT performance. IT governance is integral to the success of enterprise governance by assuring efficient and effective measurable improvements in related enterprise processes. IT governance enables the enterprise to take full advantage of its information, thereby maximising benefits, capitalising on opportunities and gaining competitive advantage.

Looking at the interplay of enterprise and IT governance processes in more detail (**figure 1**), enterprise governance, the system by which entities are directed and controlled, drives and sets IT governance. At the same time, IT should provide critical input to, and constitute an important component of, strategic plans. IT may in fact influence strategic opportunities outlined by the enterprise.

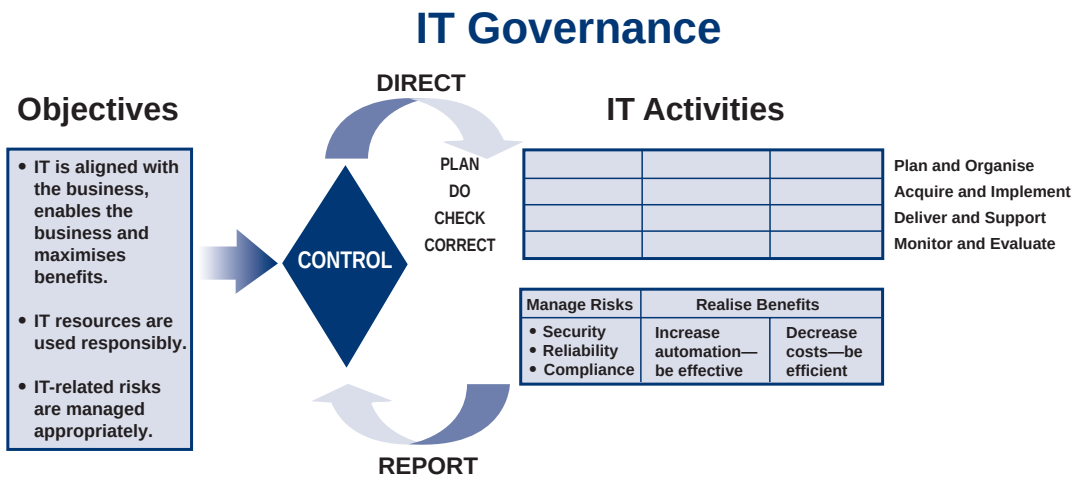
Figure 1—Enterprise Governance and IT Governance



Well-managed enterprises employ generally accepted best practices to ensure that the enterprise is achieving its strategic and operational goals. Achieving those goals requires an entity to take on some level of risk—there can be no reward without some level of risk. The entity institutes controls over strategy and operations to manage its risk and assist in the achievement of its goals and strategies. From these objectives flows the organisation's direction, which dictates certain enterprise activities, using the enterprise's resources. The results of the enterprise activities are measured and reported on, providing input to the constant revision and maintenance of the controls, beginning the cycle again.

The management of IT is also governed by best practices to ensure that the enterprise's information and related technology support its business objectives, its resources are used responsibly and its risks are managed appropriately. These practices form a basis for direction of IT activities, which can be characterised as plan and organise, acquire and implement, deliver and support, and monitor and evaluate, for the dual purposes of managing risks (to gain security, reliability and compliance) and realising benefits (increasing effectiveness and efficiency). Reports are issued on the outcomes of IT activities, which are measured against the various practices and controls, and then the cycle begins again. This cycle is illustrated in **figure 2**.

Figure 2—IT Governance Cycle

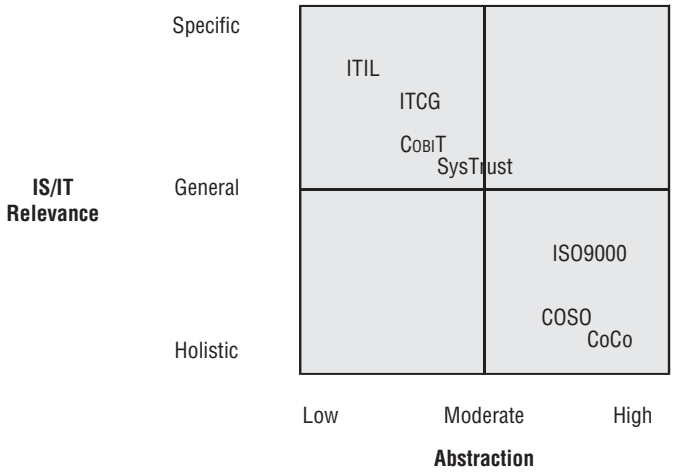


In view of these ongoing changes, the development of this framework for IT control objectives and the continued applied research in IT controls, based on this framework, are cornerstones for effective progress in the field of information and related technology controls.

Overall business control models, such as COSO (Committee of Sponsoring Organisations of the Treadway Commission, *Internal Control—Integrated Framework*, 1992, the *COSO Enterprise Risk Management Framework*, 2004) in the US, Turnbull in the UK, CoCo in Canada and King in South Africa have been developed and published. As well, a number of IT-only control models exist, such as the Security Code of Conduct from the Department of Trade and Industry (DTI), UK, Information Technology Control Guidelines from the Canadian Institute of Chartered Accountants (CICA), Canada, and the Security Handbook from the National Institute of Standards and Technology (NIST), USA. However, these focused control models do not provide a comprehensive and usable control model over IT that is in support of business processes. The purpose of COBIT is to bridge this gap by providing a foundation that is closely linked to business objectives while focusing on IT.

Most closely related to COBIT from an IT perspective is the *SysTrust™ Principles and Criteria* for systems reliability. SysTrust is an authoritative issuance of both the Assurance Services Executive Committee of the American Institute of Certified Public Accountants (AICPA) in the US and the Assurance Services Development Board of CICA in Canada, based in part on the COBIT control objectives. SysTrust is designed to increase the comfort of management, customers and business partners with the systems that support a business or a particular activity. The SysTrust service entails the public accountant providing an assurance service in which he/she evaluates and tests whether a system is reliable when measured against four essential principles: availability, security, integrity and maintainability. Other control and governance models are mapped in **figure 3**; they include IT Infrastructure Library (ITIL), Information Technology Control Guidelines (ITCG), International Organisation for Standardisation's ISO9000, COSO report (a report on *Internal Control—An Integrated Framework*, sponsored by COSO) and Criteria of Control (CoCo), published by the CICA.

Figure 3—Models of Control and Governance



Adapted from Gartner Group, June 2003

The main focus of COBIT is the development of clear policies and good practices for security and control in IT for worldwide endorsement by commercial, governmental and professional organisations. Its primary goal is the development of control objectives primarily from the business objectives and needs perspective. This approach is compliant with the COSO perspective, which is first and foremost a management framework for internal controls. Subsequently, audit objectives and guidelines were developed from the control objectives (certification of financial information, certification of internal control measures, efficiency and effectiveness, etc.) perspective.

What a Chief Finance Officer (CFO) of an Energy Company Thinks of COBIT

A US energy company adopted COBIT in response to the Sarbanes-Oxley regulations. It had been looking for a structure, and instead of developing its own control framework, it preferred to adopt an internationally accepted framework—COBIT. The CFO, who is a member of the organisation's IT steering committee, stated: "The board of directors is responsible for our internal controls. They have authorised the board's audit committee to make sure that we are doing our job. The audit committee has authorised the C-suite (CEO, CFO, COO, etc.) to make sure we are doing our job, and the C-suite has asked this IT steering committee to make sure we have adequate internal controls for IT. The IT steering committee, in return, is asking the CIO and his management team to make us comfortable that this is so with regards to IT, and we are going to use COBIT to do it."

COBIT AUDIENCE: MANAGEMENT, USERS AND AUDITORS

COBIT is designed to be used by three distinct audiences:
- **Management**—To help them balance risk and control investment in an often unpredictable IT environment
- **Users**—To obtain assurance on the security and controls of IT services provided by internal or third parties
- **Auditors**—To provide a framework to assist them to come to an opinion on the level of assurance on the particular subject matter being audited and/or provide advice to management on internal controls

CISA and CISM Certification
For the above target audiences, ISACA has also developed certification programs. After passing an exam and meeting the necessary experience requirements, an internationally accepted certification can be obtained. The Certified Information Systems Auditor™ (CISA®) exam measures excellence in the area of IS auditing, control and security. The Certified Information Security Manager® (CISM®) is for the individual who must maintain a view of the big picture by managing, designing, overseeing and assessing an enterprise's information security. For more information on these programmes, please visit *www.isaca.org*.

COBIT FRAMEWORK SPECIFICS

To fully understand the COBIT framework, the following definitions are provided. **Control** is adapted from the COSO report (*Internal Control—Integrated Framework*) and **IT control objective** is adapted from the Systems Auditability and Control (SAC) Report, The Institute of Internal Auditors (IIA) Research Foundation, 1991 and 1994.

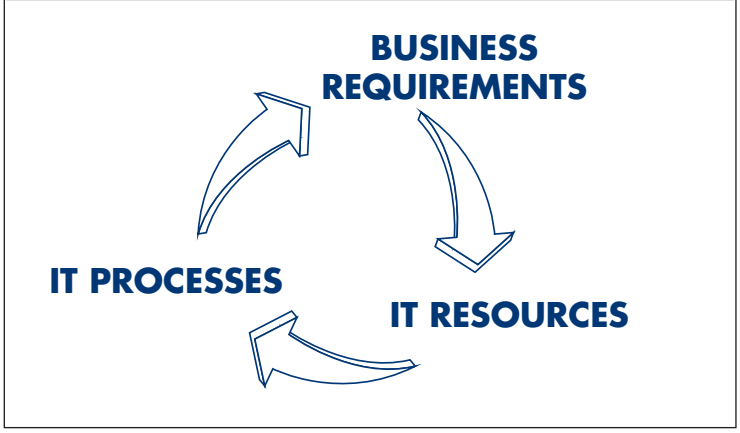
"Control" is defined as the policies, procedures, practices and organisational structures designed to provide reasonable assurance that business objectives will be achieved and undesired events will be prevented or detected and corrected.

"IT control objective" is defined as a statement of the desired result or purpose to be achieved by implementing control procedures in a particular IT activity.

"IT governance" is defined as a structure of relationships and processes to direct and control the enterprise in order to achieve the enterprise's goals by adding value while balancing risk vs. return over IT and its processes.

There are two distinct classes of control models currently available: those of the business control model class (e.g., COSO and CoCo) and the more focused control models for IT (e.g., DTI). COBIT aims to bridge the gap that exists between the two. COBIT is therefore positioned to be more comprehensive for management and to operate at a higher level than pure technology standards for information systems management.

Figure 4—Concepts That Underpin COBIT



The underpinning concept of the COBIT framework (**figure 4**) is that control in IT is approached by concentrating on information that is needed to support the business objectives or requirements, and by looking at information as being the result of the combined application of IT-related resources that need to be managed by IT processes.

CobiT

To satisfy business objectives, information needs to conform to certain criteria. These criteria are referred to, in CobiT, as business requirements for information. In establishing the list of those requirements, CobiT combines the principles embedded in existing and known reference models.

Quality requirements include:
- Quality
- Cost
- Delivery

Fiduciary requirements (COSO) include:
- Effectiveness and efficiency of operations
- Reliability of information
- Compliance with laws and regulations

Security requirements include:
- Confidentiality
- Integrity
- Availability

Quality has been retained primarily for its negative aspect (e.g., no faults and reliability), which is also captured to a large extent by the integrity criterion. The positive but less tangible aspects of quality (style, attractiveness, look and feel, performing beyond expectations, etc.) were, for a time, not being considered from an IT control objectives point of view. The premise is that the first priority should go to properly managing the risks as opposed to the opportunities. The usability aspect of quality is covered by the effectiveness criterion. The delivery aspect of quality was considered to overlap with the availability aspect of the security requirements and also, to some extent, effectiveness and efficiency. Finally, cost is also considered to be addressed by efficiency.

CobiT did not attempt to reinvent the wheel for the fiduciary requirements; COSO's definitions for effectiveness and efficiency of operations, reliability of information and compliance with laws and regulations were used. However, reliability of information was expanded to include all information—not just financial information.

With respect to the security requirements, CobiT identified confidentiality, integrity and availability as the key elements. These same three elements, it was found, are used worldwide in describing IT security requirements.

Starting the analysis from the broader quality, fiduciary and security requirements, seven distinct, certainly overlapping, categories were extracted. CobiT's working definitions for each follow:
- **Effectiveness**—Deals with information being relevant and pertinent to the business process as well as being delivered in a timely, correct, consistent and usable manner
- **Efficiency**—Concerns the provision of information through the optimal (most productive and economical) use of resources
- **Confidentiality**—Concerns the protection of sensitive information from unauthorised disclosure
- **Integrity**—Relates to the accuracy and completeness of information as well as to its validity in accordance with business values and expectations
- **Availability**—Relates to information being available when required by the business process now and in the future. It also concerns the safeguarding of necessary resources and associated capabilities.

- **Compliance**—Deals with complying with those laws, regulations and contractual arrangements to which the business process is subject, i.e., externally imposed business criteria
- **Reliability of information**—Relates to the provision of appropriate information for management to operate the entity and for management to exercise its financial and compliance reporting responsibilities

How a Major Canadian Financial Group Identifies and Uses the Information Criteria

A major Canadian financial group is planning for the implementation of a portal toward its customers. The business case for this e-business project states the following justifications, amongst others. The portal will:

- Reduce back-office costs by introducing self-service to the customers
- Provide a powerful data access tool to call centre support staff

The effectiveness in this situation relates to the accessibility and usability of the functions to the target audiences. These become the measures of success that enable the business to achieve its value proposition and become the key IT measures for the project (at least in this dimension of the project). Management then selects specific measures that indicate the achievement of these goals. The belief is that if these goals are achieved, then the take-up rates of customers will be sufficient to offload and streamline work to produce the economies built into the business case.

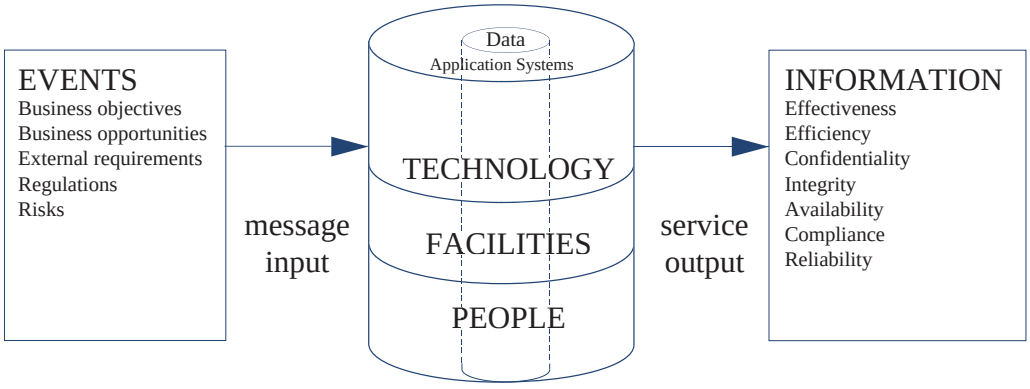
As identified in **figure 4**, there is a set of IT resources needed to help meet business requirements. The resources are:

- **Data**—Objects in their widest sense (i.e., external and internal), structured and nonstructured, graphics, sound, etc.
- **Application systems**—Understood to be the sum of manual and programmed procedures
- **Technology**—Hardware, operating systems, database management systems, networking, multimedia, etc.
- **Facilities**—All the resources to house and support information systems
- **People**—Staff skills, awareness and productivity to plan, organise, acquire, deliver, support, monitor and evaluate information systems and services

Money or capital was not retained as an IT resource for classification of control objectives because it can be considered as being the investment into any of the above resources. It should also be noted that the framework does not specifically refer to documentation of all material matters relating to a particular IT process. As a matter of good practice, documentation is considered essential for good control; therefore, lack of documentation would be cause for further review and analysis for compensating controls in any specific area under review.

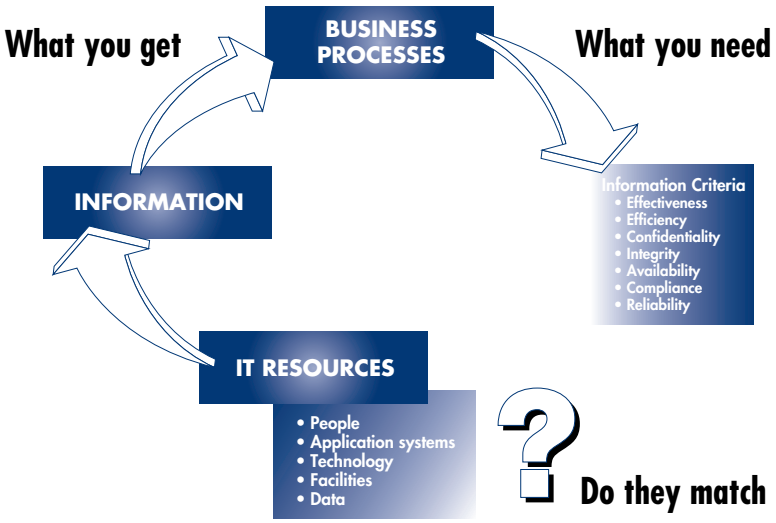
Another way of looking at the relationship of IT resources to the delivery of services is depicted in **figure 5**.

Figure 5—Relationship Between IT Resources and Delivery of Services



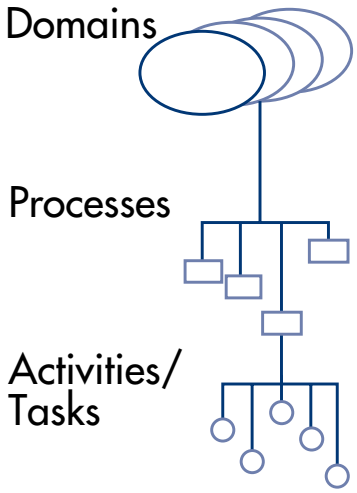
How then can organisations satisfy themselves that the information they get exhibits the characteristics they need? This is where a sound framework of IT control objectives is required. **Figure 6** illustrates this concept.

Figure 6—Framework of IT Control Objectives



The CobiT framework consists of high-level control objectives and an overall structure for their classification. The underlying theory for the classification is that there are, in essence, three levels of IT efforts when considering the management of IT resources (see **figure 7**). *First*, beginning at the bottom and working up, there are the activities and tasks needed to achieve a measurable result. Activities have a life-cycle concept, while tasks are more discrete. The life-cycle concept has typical control requirements different from discrete activities. *Second*, processes are then defined one layer up as a series of joined activities or tasks with natural (control) breaks. *Third*, at the highest level, processes are naturally grouped together into domains. Their natural grouping is often confirmed as responsibility domains in an organisational structure and is in line with the management cycle or the life cycle applicable to IT.

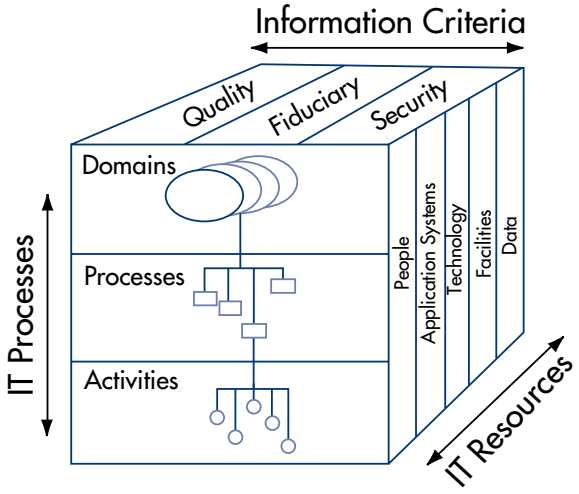
Figure 7—CobiT Domains, Processes and Activities



Thus, the conceptual framework can be approached from three vantage points:
- Information criteria
- IT resources
- IT processes

These three vantage points are depicted in the COBIT Cube (**figure 8**).

Figure 8—COBIT Cube: Processes, Resources and Information Criteria



With this framework, the domains are identified using wording that management would use in the day-to-day activities of the organisation. Thus, four broad domains are identified: plan and organise, acquire and implement, deliver and support, and monitor and evaluate.

Definitions for the four domains identified for the high-level classification are:
- **Plan and organise**—This domain covers strategy and tactics, and concerns the identification of the way IT can best contribute to the achievement of the business objectives. Furthermore, the realisation of the strategic vision needs to be planned, communicated and managed for different perspectives. Finally, a proper organisation as well as technological infrastructure must be put in place.
- **Acquire and implement**—To realise the IT strategy, IT solutions need to be identified, developed or acquired, as well as implemented and integrated into the business process. In addition, changes in and maintenance of existing systems are covered by this domain to make sure that the life cycle is continued for these systems.
- **Deliver and support**—This domain is concerned with the actual delivery of required services, which range from traditional operations over security and continuity aspects to training. In order to deliver services, the necessary support processes must be set up. This domain includes the actual processing of data by application systems, often classified under application controls.
- **Monitor and evaluate**—All IT processes need to be regularly assessed over time for their quality and compliance with control requirements. This domain thus addresses management's oversight of the organisation's control process and independent assurance provided by internal and external audit or obtained from alternative sources.

The IT processes identified in COBIT can be applied at different levels within an organisation. For example, some of these processes will be applied at the enterprise level, others at the IT function level and still others at the business process owner level.

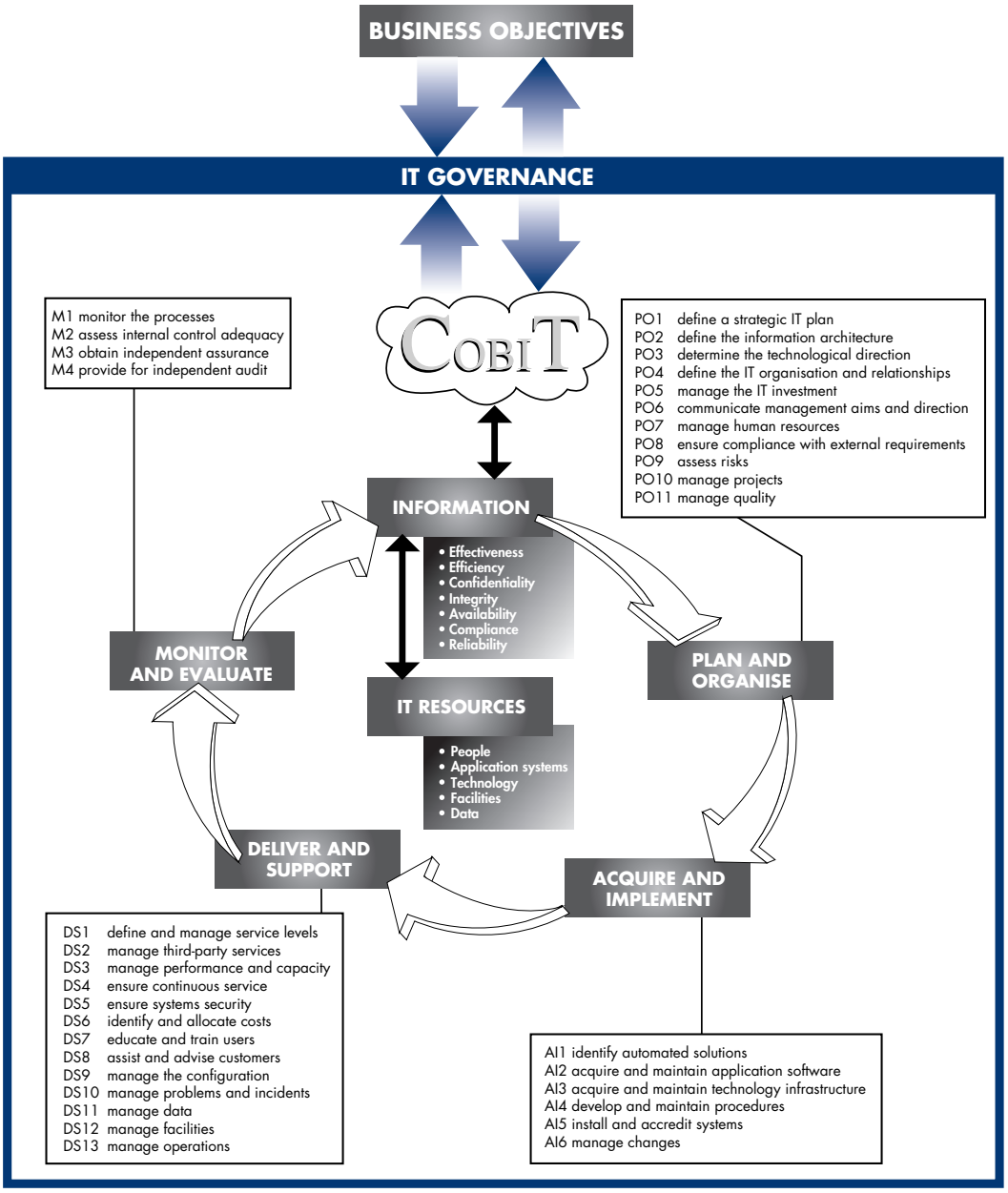
It is clear that the control measures over the IT processes will not necessarily satisfy all the different business requirements for information to the same degree. This is indicated in **figure 14** by using primary (P), secondary (S) or blank indicators:

- **Primary**—The degree to which the defined control objective directly impacts the information criterion concerned
- **Secondary**—The degree to which the defined control objective satisfies only to a lesser extent or indirectly the information criterion concerned
- **Blank**—Could be applicable; however, requirements are more appropriately satisfied by another criterion in this process and/or by another process.

Similarly, a particular control measure does not necessarily impact the different IT resources to the same degree. Therefore, the COBIT framework specifically indicates the applicability of the IT resources that are specifically managed by the process under consideration and not just those that merely take part in the process (see **figure 14**). This classification is made within the COBIT framework based on a rigorous process of input from researchers, experts and reviewers, using the strict definitions previously indicated.

In summary, in order to provide the information that the organisation needs to achieve its objectives, IT governance must be exercised by the organisation to ensure that IT resources are managed by a set of naturally grouped IT processes. **Figure 9** illustrates this concept.

Figure 9—CobiT Framework



COBIT FAMILY OF PRODUCTS

COBIT provides several products that describe the different COBIT components in detail. The following section contains a brief explanation of the most important products, using the process DS2 *manage third-party services* for all the product examples, and then a sample of each.

CONTROL OBJECTIVES

COBIT provides a set of 34 high-level control objectives, one for each of the IT processes, grouped into four domains: plan and organise, acquire and implement, deliver and support, and monitor and evaluate. This structure covers all aspects of information and the technology that supports it. By addressing these 34 high-level control objectives, the business process owner can ensure that an adequate control system is provided for the IT environment. Each high-level control objective is subdivided in a list of detailed control objectives. In total, COBIT contains 318 detailed control objectives over all the 34 IT processes. **Figure 10** provides an example of the high-level control objective and a detailed control objective.

Figure 10—Example of a Control Objective

High-level control objective for DS2 *manage third-party services*

Control over the IT process of managing third-party services

that satisfies the business requirement to ensure that roles and responsibilities of third parties are clearly defined, adhered to and continue to satisfy requirements

is enabled by control measures aimed at the review and monitoring of existing agreements and procedures for their effectiveness and compliance with organisation policy

and takes into consideration

- Third-party service agreements
- Contract management
- Nondisclosure agreements
- Legal and regulatory requirements
- Service delivery monitoring and reporting
- Enterprise and IT risk assessments
- Performance rewards and penalties
- Internal and external organisational accountability
- Analysis of cost and service level variances

Detailed control objective for DS2 *manage third-party services*

Supplier interfaces

Management should ensure that all third-party providers' services are properly identified and that the technical and organisational interfaces with suppliers are documented.

CONTROL PRACTICES

Control practices expand the capabilities of COBIT by providing the practitioner with an additional level of detail. The COBIT IT processes, business requirements and detailed control objectives define *what* needs to be done to implement an effective control structure. The IT control practices provide the more detailed *how* and *why* needed by management, service providers, end users and control professionals to implement highly specific controls based on an analysis of operational and IT risks. **Figure 11** provides an example control practice, again using DS2 *Manage third-party services*.

Figure 11—Example Control Practice

Control practice for the detailed control objective *supplier interfaces* of process DS2 *manage third-party services*

Why Do It?
Identifying and defining technical and organisational interfaces provided by third-party suppliers in line with the control practices will:
- Promote relationships that support the overall organisational objectives (both business and IT)
- Facilitate effective and efficient communication (including problem resolution) between organisations to help maintain effective service delivery
- Ensure that the ownership of those elements on each side of the boundary between the organisation and third-party service provider is clear, and therefore avoid gaps or overlaps in responsibility that may lead to loss of service or operational inefficiencies

Control Practices
1. Policy and procedures in relation to maintaining a register of key suppliers to the IT function are developed. The register details the name of supplier and nature, scope and purpose of relationship. Procedures link to, and should be integrated with, procurement and configuration management procedures.
2. The register of IT suppliers is periodically reviewed to ensure that it remains current.
3. Policy and procedures in relation to maintaining a register of system interfaces are developed. The register details the name of interface, systems it relates to and purpose (in both business and IT terms). Procedures link to, and should be integrated with, configuration and change management procedures.

AUDIT GUIDELINES

Management needs assurance that the desired IT goals and objectives are being met and key controls are being addressed. The audit guidelines outline and suggest the assessment activities to be performed corresponding to each of the 34 high-level IT control objectives, providing helpful guidance on who to interview; what questions to ask; and how to evaluate control, assess compliance and finally substantiate the risk of any identified controls *not* being met. This publication provides invaluable guidance for the audit team, and a structured audit approach linked to a framework that IT people can understand, which facilitates a shared identification of control priorities and improvements.

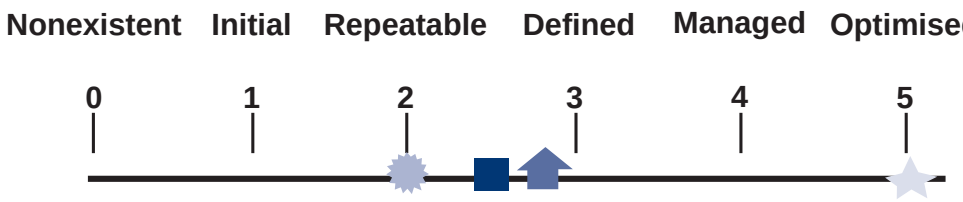
MANAGEMENT GUIDELINES

The CobiT management guidelines provide the vital link between IT control and IT governance. They are action-oriented and generic, and provide management direction for getting the enterprise's information and related processes under control, monitoring achievement of organisational goals, monitoring and improving performance within each IT process, and benchmarking organisational achievement. They help provide answers to typical management questions, such as:
- How far should we go in controlling IT, and is the cost justified by the benefit?
- What are the indicators of good performance?
- What are the critical success factors?
- What are the risks of not achieving our objectives?
- What do others do?
- How do we measure and compare?

The management guidelines include:

- **Maturity models**—Maturity models for control over IT processes consist of a method of scoring, so an organisation can grade its maturity for an IT process, from nonexistent to optimised, using a graduated scale from 0 to 5. This approach, as illustrated in **figure 12**, has been derived from the maturity model that the Software Engineering Institute (SEI) defined for the maturity of the software development capability. By developing and actively using these levels for each of COBIT's 34 IT processes, management can map:
  – The current status of the organisation—Where the organisation is today
  – The current status of (best-in-class in) the industry—The comparison
  – The current status of international standards—Additional comparison
  – The organisation's strategy for improvement—Where the organisation wants to be

Figure 12—Maturity Model



LEGEND FOR SYMBOLS USED

- Enterprise Current Status
- International Standard Guidelines
- Industry Best Practice
- Enterprise Strategy

LEGEND FOR RANKINGS USED

0	Nonexistent	– Management processes are not applied at all.
1	Initial	– Processes are *ad hoc* and disorganised.
2	Repeatable	– Processes follow a regular pattern.
3	Defined	– Processes are documented and communicated.
4	Managed	– Processes are monitored and measured.
5	Optimised	– Best practices are followed and automated.

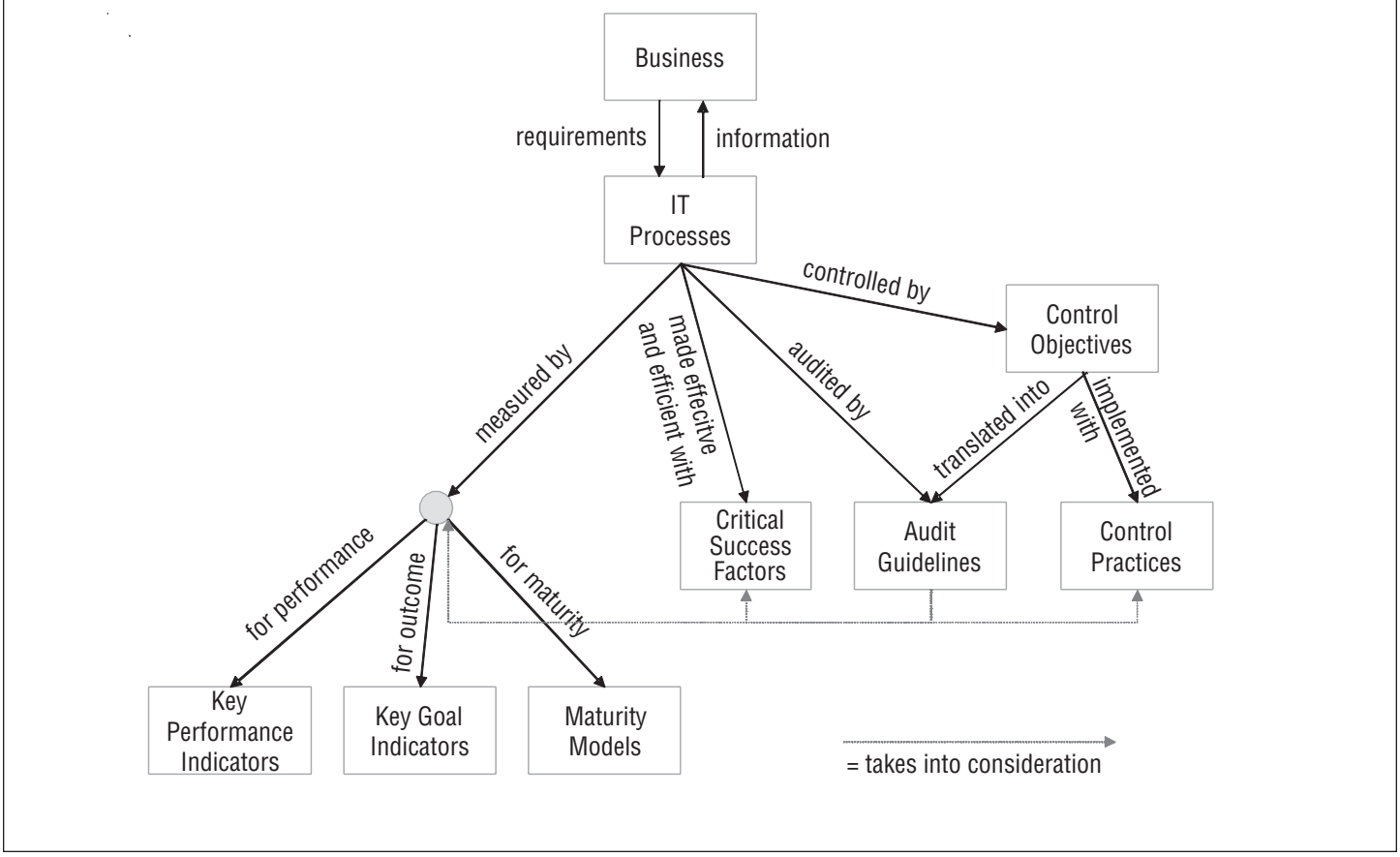
- **Critical success factors (CSFs)**—CSFs define the most important issues or actions for management to consider or undertake to achieve control over and within the IT processes. They must be management-oriented implementation guidelines and identify the most important things to do, strategically, technically, organisationally or procedurally. For example, CSFs include:
  – IT processes are defined and aligned with the IT strategy and the business goals.
  – The customers of the process and their expectations are known.
  – Processes are scalable and their resources are appropriately managed and leveraged.
- **Key goal indicators (KGIs)**—KGIs define measures that tell management, after the fact, whether an IT process has achieved its business requirements. For example, KGIs include:
  – Achieving targeted return on investment or business value benefits
  – Enhanced performance management
  – Reduced IT risks
- **Key performance indicators (KPIs)**—KPIs define measures to determine how well the IT process is performing in enabling the goal to be reached. They are lead indicators of whether a goal will likely be reached or not, and are good indicators of capabilities, practices and skills. For example, KPIs include:
  – Reduced cycle times (i.e., responsiveness of IT production and development)
  – Service availability and response times
  – Number of staff trained in new technology and customer service skills

COBIT and the Balanced Scorecard
The KGIs and KPIs provided in COBIT offer useful information to help build a balanced scorecard for the IT department or specific domains or processes of IT. The KGIs and KPIs provide input to define the metrics in the different perspectives of the balanced scorecard (financial perspective, customer perspective, internal processes, learning and innovating). It is important not only to define the metrics in each of the perspectives, but also to identify causal relationships between the KPIs and KGIs. KGIs, such as "customer satisfaction that the service level meets expectations," without KPIs, such as "the time lag of resolution of a service level change request," do not communicate how the outcomes are to be achieved. And KPIs without KGIs may lead to significant investments without a proper measurement indicating whether the chosen service level management (SLM) strategy is effective. A good balanced scorecard, therefore, contains a mix of related KGI and KPIs.

Major Transportation Organisation Uses Balanced Scorecard and COBIT to Manage IT Productivity
De Lijn is a major publicly owned transport group in Belgium employing nearly 7,000 people. The Gartner Group reports that De Lijn uses the balanced scorecard approach and COBIT to improve customer responsiveness and the productivity of the IT group.

Figure 13 demonstrates how all the COBIT components described above link together.

Figure 13—COBIT Components Linked



CobiT BUSINESS OBJECTIVE ORIENTATION

CobiT is aimed at addressing business objectives. The control objectives make a clear and distinct link to business objectives to support significant use outside the assurance community. Control objectives are defined in a process-oriented manner following the principle of business reengineering. At identified domains and processes, a high-level control objective is identified and rationale is provided to document the link to the business objectives. In addition, considerations and guidelines are provided to define and implement the IT control objective.

The classification of domains where high-level control objectives apply (domains and processes) are an indication of the business requirements for information in that domain, as well as the IT resources primarily impacted by the control objectives. Together, they form the CobiT framework. The framework is based on the research activities that have identified 34 high-level control objectives and 318 detailed control objectives. The framework was exposed globally to the IT industry and the audit profession to allow an opportunity for review, challenge and comment. The insights gained have been, and will continue to be, appropriately and consistently incorporated.

CobiT Case Study: South African Breweries Limited

South African Breweries Limited (SAB Ltd.) manufactures and distributes beer and nonalcoholic beverages in Europe, Asia and Africa. More than 200 of the organisation's 7,000 employees work in the information systems field. After learning about CobiT from the Gartner Group, SAB Ltd. used CobiT to develop an IT and enterprise architecture strategy document. The SAB Ltd. approach fostered partnering opportunities between IS audit and the IT community. The IS audit team implemented value-added components to the reviews, which allowed a more rigorous interpretation of IT risk. Once the business benefits of CobiT were communicated, senior business executives realised the framework could help determine accountability for processes and improve IT governance. By using the framework as the basis for an accountability matrix, SAB Ltd. began achieving a role-based IT organisation with defined process measures to ensure customer value.

COBIT SUMMARY TABLE

As discussed earlier in the text, **figure 14** provides an indication, by IT process and domain, of which information criteria are impacted by the high-level control objectives and which IT resources are applicable. The table maps information criteria for each of the 34 IT processes (control objectives).

Figure 14—COBIT Summary Table

DOMAIN		PROCESS	Information Criteria							IT Resources				
			Effectiveness	Efficiency	Confidentiality	Integrity	Availability	Compliance	Reliability	People	Applications	Technology	Facilities	Data
Plan and Organise	PO1	Define a strategic IT plan	P	S						✔	✔	✔	✔	✔
	PO2	Define the information architecture	P	S	S	S					✔			✔
	PO3	Determine technological direction	P	S								✔	✔	
	PO4	Define the IT organisation and relationships	P	S						✔				
	PO5	Manage the IT investment	P	P					S	✔	✔	✔	✔	
	PO6	Communicate management aims and direction	P					S		✔				
	PO7	Manage human resources	P	P						✔				
	PO8	Ensure compliance with external requirements	P					P	S	✔	✔			✔
	PO9	Assess risks	P	S	P	P	P	S	S	✔	✔	✔	✔	✔
	PO10	Manage projects	P	P						✔	✔	✔	✔	
	PO11	Manage quality	P	P		P			S	✔	✔	✔	✔	
Acquire and Implement	AI1	Identify automated solutions	P	S							✔	✔	✔	
	AI2	Acquire and maintain application software	P	P		S		S	S		✔			
	AI3	Acquire and maintain technology infrastructure	P	P		S						✔		
	AI4	Develop and maintain procedures	P	P		S		S	S	✔	✔	✔	✔	
	AI5	Install and accredit systems	P			S	S			✔	✔	✔	✔	✔
	AI6	Manage changes	P	P		P	P		S	✔	✔	✔	✔	✔
Deliver and Support	DS1	Define and manage service levels	P	P	S	S	S	S	S	✔	✔	✔	✔	✔
	DS2	Manage third-party services	P	P	S	S	S	S	S	✔	✔	✔	✔	✔
	DS3	Manage performance and capacity	P	P			S				✔	✔	✔	
	DS4	Ensure continuous service	P	S			P			✔	✔	✔	✔	✔
	DS5	Ensure systems security			P	P	S	S	S	✔	✔	✔	✔	✔
	DS6	Identify and allocate costs		P					P	✔	✔	✔	✔	✔
	DS7	Educate and train users	P	S						✔				
	DS8	Assist and advise customers	P	P						✔	✔			
	DS9	Manage the configuration	P				S		S		✔	✔	✔	
	DS10	Manage problems and incidents	P	P			S			✔	✔	✔	✔	✔
	DS11	Manage data				P			P					✔
	DS12	Manage facilities				P	P						✔	
	DS13	Manage operations	P	P		S	S			✔	✔		✔	✔
Monitor and Evaluate	M1	Monitor the processes	P	P	S	S	S	S	S	✔	✔	✔	✔	✔
	M2	Assess internal control adequacy	P	P	S	S	S	P	S	✔	✔	✔	✔	✔
	M3	Obtain independent assurance	P	P	S	S	S	P	S	✔	✔	✔	✔	✔
	M4	Provide for independent audit	P	P	S	S	S	P	S	✔	✔	✔	✔	✔

REVIEW QUESTIONS

1. How does the cycle of plan, do, check and correct relate to IT governance?

2. Describe the similarities and differences between CoCo or COSO and COBIT. Could an entity employ both CoCo or COSO *and* COBIT? Should an entity employ both CoCo or COSO *and* COBIT?

3. Describe the target audience of COBIT.

4. Describe the seven information criteria that COBIT is designed to address.

5. Discuss the five IT resources recognised by the COBIT framework.

6. What is the difference between an audit guideline and a management guideline? Why should there be separate guidelines in the COBIT framework?

7. What is the difference between the general concept of control and control in the IT environment?

8. Give two examples of IT domains and explain each.

9. What is the difference between a key goal indicator and a key performance indicator?

10. What is a maturity model? Invent a maturity model for a knowledge domain outside of information technology (e.g., for a student, sports or cultural activity or organisation).

11. What is an IT process? Give two examples of IT processes.

CHAPTER 2: COBIT COMPONENTS FOR IT PROCESS DS2

The objective of this chapter is to demonstrate how to use the COBIT framework. It begins with a navigational outline of the COBIT framework, which shows how to navigate through the COBIT product set. Next, all the COBIT components of the COBIT process DS2 *manage third-party services* are explained and linked to each other.

COBIT FRAMEWORK NAVIGATION

The COBIT framework defines 34 IT processes divided into four IT domains: Plan and Organise (PO), Acquire and Implement (AI), Deliver and Support (DS), and Monitor and Evaluate (M). For each of the 34 IT processes, COBIT provides control objectives, control practices, management guidelines and audit guidelines.

For each IT process, the high-level control objectives section presents control statements, business requirements, enablers and considerations. The domain indicator ("PO" for Plan and Organise, "AI" for Acquire and Implement, "DS" for Deliver and Support, and "M" for Monitor and Evaluate) is shown at top left in this high-level control objective section. The applicable information criteria and IT resources managed are shown in **figures 15** and **16.**

The remainder of this chapter, focused on *manage third-party services*, is organised as follows:
- Concept and importance of the process
- Control objective
- Control practice
- Audit guidelines
- Management guidelines
- Chapter review questions

Figure 15—COBIT Waterfall

The COBIT framework has been limited to high-level control objectives in the form of a business need within a particular IT process, the achievement of which is enabled by a control statement, for which consideration should be given to potentially applicable controls.

The control objectives have been organised by process/activity, but navigation aids have been provided not only to facilitate entry from any one vantage point, but also to facilitate combined or global approaches, such as installation/implementation of a process, global management responsibilities for a process and the use of IT resources by a process.

It should also be noted that the control objectives have been defined in a generic way, i.e., not depending on the technical platform, while accepting the fact that some special technology environments may need separate coverage for control objectives.

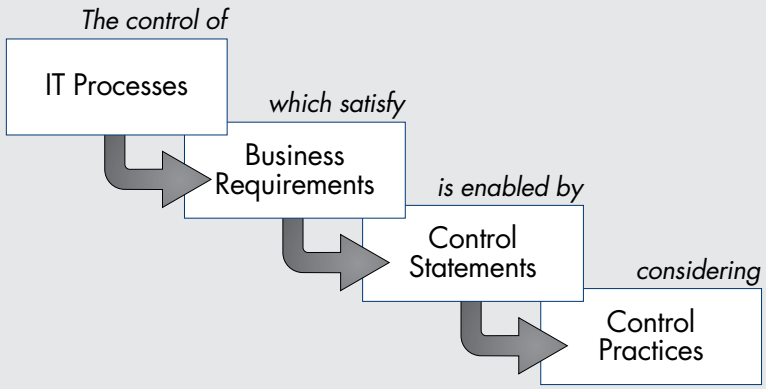
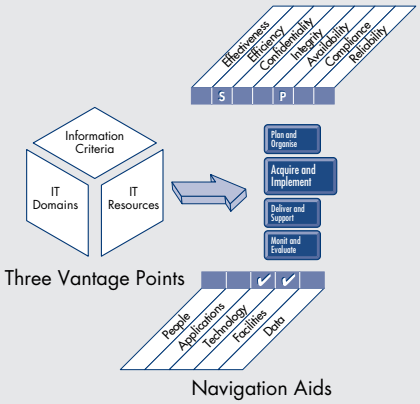


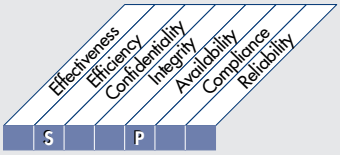
Figure 16—CobiT Navigation Aids

To facilitate efficient use of the control objectives in support of the different vantage points, some navigation aids are provided as part of the presentation of the high-level control objectives. For each of the three dimensions along which the CobiT framework can be approached—processes, IT resources and information criteria—a navigation aid is provided.

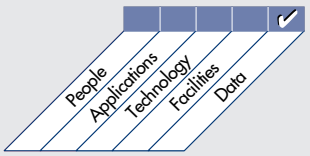


IT domains are identified by this icon in the Upper Right Corner of each page in the control objectives section, with the domain under review highlighted and enlarged.

The cue to information criteria is provided in the Upper Left Corner in the control objectives section by means of this matrix, which identifies which criteria are applicable to each high-level control objective and to which degree (primary or secondary).



A second matrix in the Lower Right Corner in the control objectives section identifies the IT resources that are specifically managed by the process under consideration—not those that merely take part in the process. For example, the *manage data* process concentrates particularly on integrity and reliability of the data resource.



CONCEPT AND IMPORTANCE OF DS2 *MANAGE THIRD-PARTY SERVICES*

Many entities now use outsourcing for support services within their IT function all the way through to complete outsourcing of all their IT functions to a third party. An entity might contract the repair and maintenance of its personal computers to a third party, place its internal and external networks in the hands of a telecommunications specialist or employ web-based software from an application service provider, such as NetSuite, that provides customer relationship management (CRM) and enterprise resource planning (ERP) functionality across the Internet. Whenever an entity employs outsourcing, it takes advantage of the benefits of scale of operations and specialist expertise of the provider. The entity can concentrate on what it does best—be it running public services in a municipality or developing and manufacturing high-performance sports equipment. Of course, outsourcing of IT services means that the entity is now dependent on the outsourcing vendor to manage operations that are likely critical to its business model. Imagine a firm that cannot access the Internet or whose e-commerce servers are no longer available to the public or its business partners. So,

management of third-party services is an important task for IT and operational management in entities that outsource services to third parties.

A Case Study of Strategic Outsourcing
CIO magazine reported on the outsourcing by Merrill Lynch, a large retail securities broker and financial services advisor in the US, of a major element of its core information technology. Thomson Financial Services now acts as the primary contractor in developing and maintaining Merrill Lynch's "wealth management workstation platform," which is used by its 14,000 financial advisors in assisting their clients. Thomson in turn subcontracts to companies such as AT&T, Cap Gemini Ernst & Young, Dell, HP, IBM and Microsoft. Merrill Lynch's contract with Thomson includes "service level agreements (SLAs), sets out performance bonuses, establishes penalties and covers more than a few other details."
Source: *CIO* Magazine, September 2003 (*www.cio.com/archive/091503/billion.html*)

CONTROL OBJECTIVES FOR DS2 *MANAGE THIRD-PARTY SERVICES*

COBIT defines one high-level control objective and from three to 30 detailed control objectives for each of the 34 IT processes. These control objectives contain statements of the desired outcomes to be achieved by implementing specific control procedures within the given IT-related activity.

A summary of the high-level and detailed control objectives for the process under review (DS2 *manage third-party services*) is shown in **figure 17**. The first part of **figure 17** shows the high-level control objective. It is clear that this high-level control objective does not necessarily satisfy the different business requirements for information (effectiveness, efficiency, confidentiality, integrity, availability, compliance, reliability) to the same degree. Therefore, the degree to which the control objective impacts the information criterion concerned is indicated on the first page as primary (P) or secondary (S). The first page also gives an overview of the IT resources that are specifically managed by the process under review.

The detailed control objectives are shown on the next part of **figure 17** and emphasise the importance of documented supplier interfaces and ownership for managing the quality of relations with third parties. Third-party contacts and outsourcing contracts should be clearly defined and mutually agreed upon, and before selection, the potential third parties should go through a quality check to make sure that they can deliver the required services. Agreements should be made regarding continuity of services and security issues. Finally, a monitoring process should be established to ensure that the services are delivered as agreed.

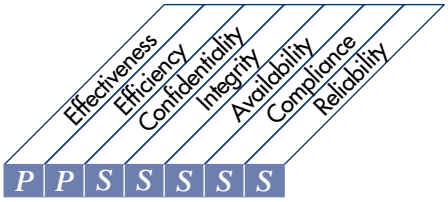
The control objectives can be used proactively by corporations to manage their third-party relationships. For example, as an entity negotiates its IT outsourcing agreements, it can use DS2 as a guide for planning the strategic and contractual relationships between the entity and the outsourcing partner(s). Of course, the systems that are put in place at the commencement of an outsourcing arrangement may not be maintained. They may no longer match changing business dynamics as the activities of the contracting entity respond to changing markets. An auditor can employ DS2 as a foundation for determining the extent of audit effort in assessing the quality of internal controls over the outsourcing agreement.

Figure 17—Control Objectives for *Manage Third-party Services*

HIGH-LEVEL CONTROL OBJECTIVE

DS2 Deliver and Support

Manage Third-party Services



Control over the IT process of

managing third-party services

that satisfies the business requirement

to ensure that roles and responsibilities of third parties are clearly defined, adhered to and continue to satisfy requirements

is enabled by

control measures aimed at the review and monitoring of existing agreements and procedures for their effectiveness and compliance with organisation policy

and takes into consideration

- Third-party service agreements
- Contract management
- Nondisclosure agreements
- Legal and regulatory requirements
- Service delivery monitoring and reporting
- Enterprise and IT risk assessments
- Performance rewards and penalties
- Internal and external organisational accountability
- Analysis of cost and service level variances

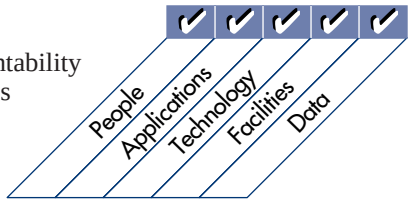


Figure 17—Control Objectives for *Manage Third-party Services*

DETAILED CONTROL OBJECTIVES

2 MANAGE THIRD-PARTY SERVICES

2.1 Supplier Interfaces

CONTROL OBJECTIVE

Management should ensure that all third-party providers' services are properly identified and the technical and organisational interfaces with suppliers are documented.

2.2 Owner Relationships

CONTROL OBJECTIVE

The customer organisation management should appoint a relationship owner who is responsible for ensuring the quality of the relationships with third-parties.

2.3 Third-party Contracts

CONTROL OBJECTIVE

Management should define specific procedures to ensure that for each relationship with a third-party service provider a formal contract is defined and agreed upon before work starts.

2.4 Third-party Qualifications

CONTROL OBJECTIVE

Management should ensure that, before selection, potential third parties are properly qualified through an assessment of their capability to deliver the required service (due diligence).

2.5 Outsourcing Contracts

CONTROL OBJECTIVE

Specific organisational procedures should be defined to ensure that the contract between the facilities management provider and the organisation is based on required processing levels, security, monitoring and contingency requirements, and other stipulations as appropriate.

2.6 Continuity of Services

CONTROL OBJECTIVE

With respect to ensuring continuity of services, management should consider business risk related to the third party in terms of legal uncertainties and the going concern concept, and negotiate escrow contracts where appropriate.

2.7 Security Relationships

CONTROL OBJECTIVE

With regard to relationships with third-party service providers, management should ensure that security agreements (e.g., nondisclosure agreements) are identified and explicitly stated and agreed to, and conform to universal business standards in accordance with legal and regulatory requirements, including liabilities.

2.8 Monitoring

CONTROL OBJECTIVE

A process for monitoring the service delivery of the third party should be set up by management to ensure continuing adherence to the contract agreements.

The Importance of Monitoring the Service Delivery of a Third Party
The following brief article, which appeared in *ComputerWorld*, demonstrates the importance of monitoring the service delivery of a third party, as is exposed by the COBIT detailed control objective 2.8.

Many outsourcing contracts contain metrics that are ineffective and insufficient.

Successful outsourcing efforts require metrics that are clearly specified, effectively monitored and consistently correlated to the needs of the business. Good metrics support your cost and service goals and are consistent with your culture. Examples include unit costs of a service (such as cost per minute, cost per help desk call) or response time per event (such as two hours to respond to a PC failure). Unfortunately, many outsourcing contracts contain metrics that are ineffective and insufficient. But even a contract that specifies excellent metrics is no guarantee of success. Metrics must be gathered, monitored and reviewed before they can be used to improve service. In many cases, the performance data is never collected, and no one even notices. Some organizations have downsized so much over the past several years that they don't have enough people to execute the measurement processes specified in their contracts. Both parties are frequently guilty of not fulfilling their sides of metrics management. Unless service levels become intolerable, many organizations believe that the efforts required to collect and manage the performance data are unwarranted. This can be a costly mistake. One company outsourced desktop procurement and management for 30,000 desktops. The multiyear contract stated that as the PC manufacturer lowered prices, the outsourcer would pass those reductions on to the company. But the customer never checked, and the outsourcer kept the difference. The company's failure to monitor its outsourcer cost it over [US] $1 million per year.

Source: *ComputerWorld*, 9 February 2004

CONTROL PRACTICES FOR DS2 *MANAGE THIRD-PARTY SERVICES*

IT control practices expand the capabilities of COBIT by providing the practitioner with an additional level of detail. The current COBIT IT processes, business requirements and detailed control objectives define *what* needs to be done to implement an effective control structure. The IT control practices provide the more detailed *why* and *how* needed by management, service providers, end users and control professionals to implement highly specific controls based on an analysis of operational and IT risks.

Figure 18 illustrates the control practices for two specific detailed control objectives, *supplier interfaces* and *owner relationships*, for the IT process *manage third-party services*. Managing third-party services is important to facilitate effective and efficient communication between organisations to help maintain effective service delivery. This can be achieved by implementing control practices, such as having a policy and procedure to maintain a register of key suppliers and ensuring that this register is continuously updated via a regular review process.

Figure 18—Control Practices for *Manage Third-party Services*

DS2.1 SUPPLIER INTERFACES

Why Do It?

Identifying and defining technical and organisational interfaces provided by third-party suppliers in line with the control practices, will:

- Promote relationships that support the overall organisational objectives (both business and IT)
- Facilitate effective and efficient communication (including problem resolution) between organisations to help maintain effective service delivery
- Ensure that the ownership of those elements on each side of the boundary between the organisation and third-party service provider is clear, and therefore avoid gaps or overlaps in responsibility that may lead to loss of service, or operational inefficiencies

Control Practices

1. Policy and procedures in relation to maintaining a register of key suppliers to the IT function are developed. The register details the name of supplier and nature, scope and purpose of the relationship. Procedures link to, and should be integrated with, procurement and configuration management procedures.
2. The register of IT suppliers is periodically reviewed to ensure that it remains current.
3. Policy and procedures in relation to maintaining a register of system interfaces are developed. The register details the name of the interface, the systems it relates to and the purpose (in both business and IT terms). Procedures link to, and should be integrated with, configuration and change management procedures.

DS2.2 OWNER RELATIONSHIPS

Why Do It?

Appointing relationship owners for IT suppliers, at an overall and individual contract level, in line with control practices will:

- Allow procurement and relationship management to be undertaken in a holistic way with each key supplier
- Facilitate proactive monitoring of service delivery performance (quality, timing and cost) and resolution of potential service delivery issues
- Ensure clarity of responsibility and decision-making authority within the procuring organisation resulting in better supplier management and consequential service delivery

Control Practices

1. Management retains accountability for provision and quality of services delivered by third parties.
2. Roles and responsibilities for management of overall supplier relationship and management of individual supplier contracts are formalised.
3. Roles are assigned to appropriate personnel based on experience and qualifications. These roles are communicated within the organisation to ensure awareness.
4. Reporting lines between the organisation and the third party, and within the organisation itself, are defined and documented.
5. Formal measures for the quality of the relationship with third parties are determined, implemented and monitored. Management agrees to specific, measurable, achievable, results-oriented and time-bound (SMART) service levels with the supplier management and assesses compliance with these SLAs with agreed frequency.

Case Study of IT Outsourcing Risks—Loss of Important Information
Dr. Larry Ponemon reports on a case study of a US-based corporation that outsourced major IT operational functions to the Ukraine. This location was chosen because:
- The workforce was well educated and the vendor had the necessary call center setup skills.
- The cost of operations was very favorable and included significant tax incentives provided by the government.
- The outsourcing industry in the Ukraine was booming.

Ponemon reports that:

> *After the decision was made, the company's legal and procurement team formulated contracts with the vendor to ensure that it took full responsibility for complying with the privacy policy, which included a strict do-not-share with third parties for secondary uses without consent, and all US regulatory requirements. The Ukraine vendor also agreed by legal contract to comply with strict data protection and information security requirements as suggested by the US Federal Trade Commission's Safeguards Rule.*

Unfortunately, after a relatively short period the company experienced many problems with billing, identity theft and fraud on customer bank accounts. According to Ponemon, a forensic expert found that the source of the information leak was in the Ukraine and undertaken by a new IT employee. Ponemon notes that:

> *While the IT employee did not have a criminal history, her husband was a convicted mobster on a US cybercrime watch list. She claimed that her company did not explain security and privacy requirements to employees. She believed that the downloading and sharing of information would not harm anyone.*

Source: *CIO* magazine, April 2004

AUDIT GUIDELINES FOR DS2 *MANAGE THIRD-PARTY SERVICES*

In addition to and corresponding with each of the 34 high-level control objectives, COBIT provides audit guidelines. The goal of these guidelines is to enable the review of IT processes against the recommended detailed control objectives. This can help the IT auditor to:
- Provide management with reasonable assurance that the control objectives are being met
- Substantiate the resulting risks, where there are significant control weaknesses
- Advise management on corrective actions

COBIT applies a generally accepted structure for performing this audit process:
1. Obtaining an understanding of business requirements, related risks and relevant control measures within the process that will be audited. A thorough understanding of the activities underlying the control objectives and the stated control measures and procedures is an essential first step in the audit process.
2. Evaluating the appropriateness of stated controls in the IT process. The appropriateness can be evaluated by considering identified criteria and industry best practices, reviewing critical success factors of the control measures and applying professional judgement of the auditor.
3. Assessing compliance by testing whether the stated controls are working as prescribed, consistently and continuously
4. Substantiating the risk of control objectives not being met by using analytical techniques and/or consulting alternative sources. The goal is to make clear the nature of the risks by, for example, shocking management into action.

The DS2 *manage third-party services* audit process illustrated in **figure 19** is typically used by an auditor to design a detailed audit programme. Obtaining an understanding of the process (policies, procedures,

responsibilities, etc.) can, for example, be achieved by interviewing the CIO, IT senior management, etc. The controls and procedures can be evaluated, for example, by checking their consistency with the general organisational policies. Compliance can be assessed by examining whether the controls are followed as prescribed and, for example, testing whether contracts contain all the prescribed elements. Finally, the risk of control objectives not being met could be substantiated by benchmarking third-party services against similar organisations or international standards.

Figure 19—Audit Guidelines for *Manage Third-party Services*

DS2 MANAGE THIRD-PARTY SERVICES

CONTROL OBJECTIVES	
1	Supplier interfaces
2	Owner relationships
3	Third-party contracts
4	Third-party qualifications
5	Outsourcing contracts
6	Continuity of services
7	Security relationships
8	Monitoring

BOTH HIGH-LEVEL AND DETAILED CONTROL OBJECTIVES ARE AUDITED BY:

Obtaining an understanding by:

▶ **Interviewing:**

Chief information officer
IT senior management
IT contract/service level administrator
IT operations management
Security officer

▶ **Obtaining:**

Organisationwide polices and procedures relating to purchased services and, in particular, third-party vendor relationships
IT policies and procedures relating to third-party relationships, vendor selection procedures, contract content of such relationships, physical and logical security, quality maintenance of vendors, contingency planning and outsourcing
List of all current third-party relationships and actual contracts associated with each
Service level reporting related to third-party relationships and services
Minutes of meetings discussing contract review, performance evaluation and relationship management
Confidentiality agreements for all third-party relationships
Security access listings with profiles and resources available to vendors

Evaluating the controls by:

▶ **Considering whether:**

IT policies and procedures relating to third-party relationships exist and are consistent with organisational general policies
Policies exist specifically addressing need for contracts, definition of content of contracts, owner or relationship manager responsible for ensuring contracts are created, maintained, monitored and renegotiated as required

Figure 19—Audit Guidelines for *Manage Third-party Services* (*cont.*)

Interfaces are defined to independent agents involved in the conduct of the project and any other parties, such as subcontractors

Contracts represent a full and complete record of third-party supplier relationships

Contracts are established for continuity of services specifically, and these contracts include contingency planning by vendor to ensure continuous service to user of services

Contract contents include at least the following:

- Formal management and legal approval
- Legal entity providing services
- Services provided
- Service level agreements both qualitative and quantitative
- Cost of services and frequency of payment for services
- Resolution of problem process
- Penalties for nonperformance
- Dissolution process
- Modification process
- Reporting of service—content, frequency and distribution
- Roles between contracting parties during life of contract
- Continuity assurances that services will be provided by vendor
- User of services and provider communications process and frequency
- Duration of contract
- Level of access provided to vendor
- Security requirements
- Nondisclosure guarantees
- Right to access and right to audit

Escrow agreements have been negotiated where appropriate

Potential third parties are properly qualified through an assessment of their capability to deliver the required service (due diligence)

Assessing the compliance by:

▶ **Testing that:**

List of contracts, and actual contracts in place, is accurate

No services are being provided by vendors not on the contract list

Providers on contracts are actually performing services defined

Provider management/owners understand their responsibilities in contracts

IT policies and procedures relating to third-party relationships exist and are consistent with organisational general policies

Policies exist specifically addressing need for contracts, definition of content of contracts, owner or relationship manager responsible for ensuring contracts are created, maintained, monitored and renegotiated as required

Contracts represent a full and complete record of third-party supplier relationships

Contracts are established for continuity of services specifically, and these contracts include contingency planning by vendor to ensure continuous service to user of services

Contract contents include at least the following:

- Formal management and legal approval
- Legal entity providing services
- Services provided
- Service level agreements both qualitative and quantitative
- Cost of services and frequency of payment for services
- Resolution of problem process
- Penalties for nonperformance

Figure 19—Audit Guidelines for *Manage Third-party Services* (*cont.*)

- Dissolution process
- Modification process
- Reporting of service—content, frequency and distribution
- Roles between contracting parties during life of contract
- Continuity assurances that services will be provided by vendor
- User of services and provider communications process and frequency
- Duration of contract
- Level of access provided to vendor
- Security requirements
- Nondisclosure guarantees
- Right to access and right to audit

Users are aware of and understand need for contract policies and contracts to provide services
Appropriate independence between vendor and organisation exists
Independence of vendor sourcing and selection processes is occurring
Security access lists include only minimum number of vendor staff as required, and access is the least needed
Access hardware and software to organisation resources are managed and controlled to minimise vendor use
Actual level of service being performed compares highly to contractual obligations
Outsourcing facilities, staff, operations and controls ensure required level of performance comparable to expectation
Continuous monitoring of service delivery by third parties is performed by management
Independent audits of contractor operations occur
Assessment reports exist for potential third parties to assess their capability to deliver the required service
History of litigation activity—past and current—exists
Interfaces to independent agents involved in the conduct of the project are documented in the contract
Contracts with private branch exchange (PBX) suppliers are covered

Substantiating the risk of control objectives not being met by:

▶ **Performing:**

Benchmarking of third-party services against similar organisations or appropriate international standards/recognised industry best practices
A detailed review of each third-party contract to determine qualitative and quantitative provisions confirming obligations are defined

▶ **Identifying:**

Provisions describing, coordinating and communicating the relationship between the provider and user of information services
Third-party invoices reflect charges accurately for selected contract services
Organisational liaison with third-party vendors ensures communication of contract issues between parties and users of services
Legal counsel and management approve all contracts
Ongoing risk assessment occurs to confirm need for relationship or need for modifying the relationship
Ongoing review and corrective action by management of contract reporting is occurring
Reasonableness of charges compared to various internal, external and industry comparable performance is evaluated
Contingency plans are in place for all contracted services, specifically disaster recovery services for the IT function
For outsourced functions, apparent shortcomings or opportunities to improve performance or reduce costs exist
Implementation of recommendations contained in independent audits of the contractor is occurring

MANAGEMENT GUIDELINES FOR DS2 *MANAGE THIRD-PARTY SERVICES*

COBIT was initially created from a control and audit perspective, which explains why the control objectives and audit guidelines were the first major components of the COBIT framework. However, ITGI identified the growing need of management for measurability of IT. To respond to this need, in 2000 ITGI developed the COBIT management guidelines with tools to assess and measure the organisation's IT environment in the 34 IT processes. These management guidelines include maturity models (MMs), CSFs, KGIs and KPIs for each process.

A maturity model is a method of scoring that enables the organisation to grade its maturity for a certain process from nonexistent (0) to optimised (5). This tool offers an easy-to-understand way to determine the "as is" and the "to be" (according to enterprise strategy) positions, and enables the organisation to benchmark itself against best practices and standard guidelines. In this way, gaps can be identified and specific actions can be defined to move towards a desired position ("to be"). When doing this maturity assessment, it is important to comply with the basic principles of maturity measurement: one can move to a higher maturity only when all conditions described in a certain maturity level are fulfilled.

The maturity model for *manage third-party services*, which is shown in **figure 20**, declares that an organisation is at maturity level 1 for this process when management is aware of the need to have documented policies and procedures for third-party service procurement and signed contracts, but the measurement of the service is informal and reactive. An organisation achieves, for example, maturity level 4 when responsibilities for contract and vendor management are assigned and when formal and standardised criteria are provided for defining scope of work, services to be provided, deliverables, etc.

The maturity model is a very useful scanning mechanism for a variety of participants in the IT governance process. When reporting to the audit committee of the board, IT management can provide a highly useful categorisation of the sophistication of controls in place for each of the processes encompassed by COBIT. For example, assume that an entity has a number of major IT outsourcing agreements that are fundamental to meeting the entity's operational objectives. If IT management or a consultant reports to the audit committee that the maturity model relating to the controls implicit in DS2 is at, say, level 2, the audit committee would likely be concerned and seek immediate improvements. Conversely, if the maturity is assessed at level 4, the audit committee would seek further improvements but in a staged and measured fashion.

COBIT management guidelines also provide critical success factors, key goal indicators and key performance indicators that can be helpful when striving for a certain maturity level, e.g., achieving maturity in the process of managing third-party services.

Critical success factors are the most important elements an organisation can target to contribute to the IT process achieving its goals. For the process under review, a good example is ensuring that third parties have a quality assurance process in place.

Key goal indicators are business-driven elements indicating *what* has to be accomplished. They represent the IT process goals. A good example of such a goal indicator for *manage third-party services* is the number of third-party contractors not meeting objectives or service levels; the number should be as low as possible.

Figure 20—Maturity Model for *Manage Third-party Services*

Control over the IT process ***manage third-party services*** with the business goal of ensuring that roles and responsibilities of third parties are clearly defined, adhered to and continue to satisfy requirements

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

1 Initial/*Ad Hoc*—Management is aware of the need to have documented policies and procedures for third-party service procurement, including having signed contracts. There are no standard terms of agreement. Measurement of the service provided is informal and reactive. Practices are dependent on the experience of the individual and the commercial effectiveness of the supplier.

2 Repeatable but Intuitive—The process for overseeing third-party service providers and the delivery of services is informal. A signed, *pro forma* contract is used with standard vendor terms and conditions and description of services to be provided. Measurements are taken, but are not relevant. Reports are available, but do not support business objectives.

3 Defined Process—Well-documented procedures are in place to govern third-party procurement, with clear processes ensuring proper vetting and negotiating with vendors. The relationship with the third party is purely a contractual one. The nature of the services to be provided is detailed in the contract and includes operational, legal and control requirements. Oversight responsibility for third-party-service delivery is assigned. Contractual terms are based on standardised templates. The business risk associated with the contract is assessed and reported.

4 Managed and Measurable—Formal and standardised criteria are established for defining scope of work, services to be provided, deliverables, assumptions, time scales, costs, billing arrangements, responsibilities, business terms and conditions. Responsibilities for contract and vendor management are assigned. Vendor qualifications and capabilities are verified. Requirements are defined and linked to business objectives. A process exists to review service performance against contractual terms, providing input to current and future third-party service delivery. Transfer pricing models are used in the procurement process. All interested parties are aware of service, cost and milestone expectations.

5 Optimised—The jointly signed contract is reviewed periodically after work starts. Responsibility for quality assurance of service delivery and vendor support is assigned. Evidence of compliance with operational, legal and control contract provisions is monitored and corrective action is enforced. The third party is subject to independent periodic review, with feedback based on the nature of the review. Selected measurements vary dynamically in response to changing business conditions. Measures support early detection of problems. Comprehensive, defined reporting is linked to the third-party compensation process. Reporting provides early warning of potential problems to facilitate timely resolution.

Key performance indicators are process-driven, focusing on the how, and indicating how well the IT process enables the goal to be reached. An example of this indicator is the number and frequency of review meetings. The more frequent the review meetings, the more likely that nonperformance is spotted and corrected. All the CSFs, KPIs and KGIs for *manage third-party services*, as identified by COBIT, are described in **figure 21**.

Figure 21—CSFs, KGIs, KPIs for *Manage Third-party Services*

DS2 Deliver and Support
Manage Third-party Services

Control over the IT process ***manage third-party services*** with the business goal of ensuring that roles and responsibilities of third parties are clearly defined, adhered to and continue to satisfy requirements

ensures delivery of information to the business that addresses the required information criteria and is measured by key goal indicators

is enabled by control measures aimed at the review and monitoring of existing agreements and procedures for their effectiveness and compliance with the organisation policy

considers critical success factors that leverage specific IT resources and is measured by key performance indicators

Information Criteria
P Effectiveness
P Efficiency
S Confidentiality
S Integrity
S Availability
S Compliance
S Reliability

(**P**) primary (**S**) secondary

IT Resources
✓ People
✓ Applications
✓ Technology
✓ Facilities
✓ Data

(✓) applicable to

Critical Success Factors

- Clearly defined service requirements and performance measures exist.
- The organisation retains accountability and control and proactively manages external services.
- The service provider has a mechanism in place to report on performance measures.
- Third-party providers have a quality assurance programme in place.
- All deliverables, including operational and performance requirements, are sufficiently defined and understood by all parties.
- Effective change procedures for service requirements and performance measures are implemented.
- Contracts are subject to successful legal review and sign-off.
- There is provision for adequate management and administration, addressing financial, operations, legal and control issues.
- The application of mutually agreed service level agreements is based on agreed-upon associated rewards and penalties.
- An internal contract manager is the single point of contact with the third party.
- A request for proposal (RFP) process exists, with preestablished and agreed evaluation criteria.
- A process is in place for classifying service problems based on their importance and the required responses.

Key Goal Indicators

- Percent of service providers with formally agreed objectives
- Percent of significant agreements for which service provider qualification reviews are undertaken
- Percent of service providers that are formally qualified
- Number of third-party contractors with well-defined goals and expected deliverables
- Mutual satisfaction with the ongoing relationship
- Number of third-party contractors not meeting objectives or service levels
- Number and cost of disputes with third parties flowing from inadequate agreements or lack of performance against adequate agreements

Key Performance Indicators

- Number and frequency of review meetings
- Number of contract amendments
- Frequency of service level reports
- Number of outstanding issues
- Time lag for clearing issues
- Percent of contracts outstanding for legal review
- Time lag since the last contract review against market conditions
- Number of service contracts not using standard terms and conditions or approved exceptions

As already demonstrated in the previous example, there is an important cause-and-effect relationship between key performance indicators and key goal indicators. KGIs, such as "number of third-party contractors not meeting objectives or service levels," without KPIs, such as "number and frequency of review meetings," do not communicate how the outcomes are to be achieved; KPIs without KGIs may lead to significant investments without a proper measurement indicating whether the chosen third-party strategy is effective. Some KPIs, of course, have a higher impact on specific KGIs compared to others. It is important to identify the most important KGIs for the specific environment and closely monitor the KPIs that contribute most to it.

REVIEW QUESTIONS

1. Is "percent of outsourcing agreements with defined service level agreements" a key goal indicator or a key performance indicator?

2. Describe the essential differences between management and audit guidelines.

3. Is "number of contractual disputes with outsourcing partners" a key goal indicator or a key performance indicator?

4. Contrast high-level control objectives and detailed control objectives.

5. Refer to the case study on "IT Outsourcing Risks—Loss of Important Information" on page 30. What detailed control objectives did the firm not follow?

6. Is "proportion of outsourced business processes covered by service level agreements" a key goal indicator or a key performance indicator?

7. Picture an entity that has SLAs on core outsourced business processes coupled with monthly reporting to senior management on all its SLAs. What maturity model level is the entity likely to have?

CHAPTER 3: COBIT COMPONENTS

This chapter contains all the COBIT components (control objectives, control practices, audit guidelines and management guidelines) of a selected group of COBIT processes:

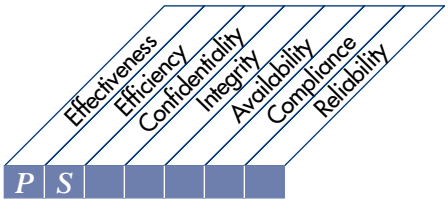
- PO1—**figures 22-25**
- PO9—**figures 26-29**
- PO10—**figures 30-33**
- AI2—**figures 34-37**
- DS5—**figures 38-41**
- DS6—**figures 42-45**
- M1—**figures 46-49**
- M2—**figures 50-53**

Figure 22—Control Objectives for *Define a Strategic Information Technology Plan*

HIGH-LEVEL CONTROL OBJECTIVE

PO1 Plan and Organise

Define a Strategic Information Technology Plan



Control over the IT process of

defining a strategic IT plan

that satisfies the business requirement

to strike an optimum balance of information technology opportunities and IT business requirements as well as ensuring its further accomplishment

is enabled by

a strategic planning process undertaken at regular intervals giving rise to long-term plans; the long-term plans should periodically be translated into operational plans setting clear and concrete short-term goals

and takes into consideration

- Enterprise business strategy
- Definition of how IT supports the business objectives
- Inventory of technological solutions and current infrastructure
- Monitoring the technology markets
- Timely feasibility studies and reality checks
- Existing systems assessments
- Enterprise position on risk, time-to-market and quality
- Need for senior management buy-in, support and critical review

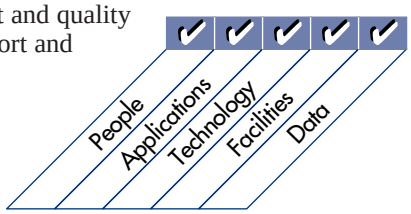


Figure 22—Control Objectives for *Define a Strategic Information Technology Plan*

DETAILED CONTROL OBJECTIVES

1 DEFINE A STRATEGIC INFORMATION TECHNOLOGY PLAN

1.1 IT as Part of the Organisation's Long- and Short-range Plan

CONTROL OBJECTIVE

Senior management is responsible for developing and implementing long- and short-range plans that fulfill the organisation's mission and goals. In this respect, senior management should ensure that IT issues as well as opportunities are adequately assessed and reflected in the organisation's long- and short-range plans. IT long- and short-range plans should be developed to help ensure that the use of IT is aligned with the mission and business strategies of the organisation.

1.2 IT Long-range Plan

CONTROL OBJECTIVE

IT management and business process owners are responsible for regularly developing IT long-range plans supporting the achievement of the organisation's overall missions and goals. The planning approach should include mechanisms to solicit input from relevant internal and external stakeholders impacted by the IT strategic plans. Accordingly, management should implement a long-range planning process, adopt a structured approach and set up a standard plan structure.

1.3 IT Long-range Planning—Approach and Structure

CONTROL OBJECTIVE

IT management and business process owners should establish and apply a structured approach regarding the long-range planning process. This should result in a high-quality plan that covers the basic questions of what, who, how, when and why. The IT planning process should take into account risk assessment results, including business, environmental, technology and human resources risks. Aspects that need to be taken into account and adequately addressed during the planning process include the organisational model and changes to it, geographical distribution, technological evolution, costs, legal and regulatory requirements, requirements of third parties or the market, planning horizon, business process reengineering, staffing, in- or outsourcing, data, application systems and technology architectures. Benefits of the choices made should be clearly identified. The IT long- and short-range plans should incorporate performance indicators and targets. The plan itself should also refer to other plans, such as the organisation quality plan and the information risk management plan.

1.4 IT Long-range Plan Changes

CONTROL OBJECTIVE

IT management and business process owners should ensure that a process is in place to modify the IT long-range plan in a timely and accurate manner to accommodate changes to the organisation's long-range plan and changes in IT conditions. Management should establish a policy requiring that IT long- and short-range plans are developed and maintained.

1.5 Short-range Planning for the IT Function

CONTROL OBJECTIVE

IT management and business process owners should ensure that the IT long-range plan is regularly translated into IT short-range plans. Such short-range plans should ensure that appropriate IT function resources are allocated on a basis consistent with the IT long-range plan. The short-range plans should be reassessed periodically and amended as necessary in response to changing business and IT conditions. The timely performance of feasibility studies should ensure that the execution of the short-range plans is adequately initiated.

continued on next page

Figure 22—Control Objectives for *Define a Strategic Information Technology Plan* (*cont.*)

1.6 **Communication of IT Plans**
CONTROL OBJECTIVE
Management should ensure that IT long- and short-range plans are communicated to business process owners and other relevant parties across the organisation.

1.7 **Monitoring and Evaluating of IT Plans**
CONTROL OBJECTIVE
Management should establish processes to capture and report feedback from business process owners and users regarding the quality and usefulness of long- and short-range plans. The feedback obtained should be evaluated and considered in future IT planning.

1.8 **Assessment of Existing Systems**
CONTROL OBJECTIVE
Prior to developing or changing the strategic or long-range IT plan, IT management should assess the existing information systems in terms of degree of business automation, functionality, stability, complexity, costs, strengths and weaknesses to determine the degree to which the existing systems support the organisation's business requirements.

Figure 23—Control Practices for *Define a Strategic Information Technology Plan*

PO1.1 IT as Part of the Organisation's Long- and Short-range Plans

Why Do It?
The consideration of IT within the organisation's long- and short-range plans will:
- Align IT with the organisation's mission and goals, increasing the likelihood of the organisation achieving its strategic objectives
- Reflect IT issues and opportunities within the long- and short-range plans of the organisation
- Aid identification and control of the investment required to provide the long- and short-range IT facilities needed to achieve core business objectives and value, whilst minimising costs
- Improve the understanding of key stakeholders within the organisation regarding the opportunities and limitations of IT within the organisation and its external business partners

Control Practices
1. Senior management establishes clear roles, responsibilities, performance measures and organisational structures for developing, implementing and maintaining the organisation's and IT's long- and short-range plans.
2. The organisation's long- and short-range plans consider business factors that could impact the focus of IT resources including, but not limited to, new markets, new competitive strategies, strategies to increase overall revenue generation, and initiatives to improve customer satisfaction and to assure customer retention.
3. The organisation's long- and short-range plans provide direction to help IT planners determine the boundaries for the IT plans. The organisation's plans consider the geographic organisational model, governance model, length of time covered by the plan, appetite for business process change, external alliances and partnerships, and available funding.

PO1.2 IT Long-range Plan

Why Do It?
The existence of an IT long-range plan will:
- Support the achievement of the organisation's mission and goals through setting strategic direction and objectives for IT development and IT operations
- Assist IT management by identifying and structuring IT strategic options
- Reduce the likelihood of an organisation investing in unnecessary IT initiatives

Control Practices
1. The senior individual within the organisation who has a clearly assigned responsibility for the management and provision of IT facilities owns the IT long-range plan.
2. The IT long-range plan is clearly aligned with the organisation's long- and short-range plans.
3. The IT long-range plan sets clear boundaries and limitations within which IT facilities will be delivered including, but not limited to, funding, delivery strategy (development and operation), sourcing models, infrastructure (complexity and charging), service needs and business process integration levels (internal and external).
4. The long-range IT plan is consistent with other organisational strategies and IT policies and procedures, such as business unit plans, a quality plan, an information risk management plan and a security policy.

PO1.3 IT Long-range Planning—Approach and Structure

Why Do It?
The utilisation of a formal approach and structure to developing an IT long-range plan will:
- Gain commitment to the contribution of IT in achieving the organisation's mission and goals from key internal and external stakeholders
- Support the development of a consistent and usable IT long-range plan
- Encourage the adoption of repeatable accepted practices, such as the consideration of risk, the setting of performance indicators against goals and actions, and the prioritisation of requirements
- Allow change factors (internal and external) to be considered and evaluated against a baseline plan by management
- Facilitate effective monitoring and evaluation of progress, benchmarking between different versions of plans, and the creation of an identifiable audit trail of plan changes

Control Practices
1. A structured and documented approach for the development and maintenance of an IT long-range plan is established. The approach makes explicit and challenges the assumptions used to create the plan and ensures that the data used in creating the plan have been validated.
2. Techniques are used and consistently applied when evaluating alternative IT strategies and tactics, including, but not limited to, financial decision support tools such as payback period, internal rate of return, return on investment, and total value of opportunity. Strategies and tactics identified as adding most value to the business are adopted.

Figure 23—Control Practices for *Define a Strategic Information Technology Plan (cont.)*

3. The attainment of widespread buy-in from key internal and external stakeholders and acceptance of the IT long-range plan through the adoption of transparent collaborative processes result in their explicit commitment to fulfilling actions required to deliver the IT plans. This may involve utilising a range of mechanisms to receive input from, and disseminate information to, parties impacted by the IT long-range plan.
4. The IT long-range plan contains defined IT goals. Processes, services and functions to deliver these goals are stated with clear explanations of rationale, ownership, benefits, timing, priorities, actions required, performance indicators and milestone target dates.
5. Appropriate internal resources and experience are used when considering factors potentially impacting the IT long-range plan, including, but not limited to, legal and regulatory developments, market changes, technological developments and third-party requirements (including business partners). External expertise is sought if not available internally.

PO1.4 IT Long-range Plan Changes

Why Do It?

A process for the modification of IT long-range plans will:
- Ensure the validity and relevance of the IT long-range plans in response to external changes and changes within the organisation or IT
- Ensure that IT long-range plans are reviewed on a regular basis

Control Practices

1. An established policy exists requiring IT plans to be developed and maintained in a timely and accurate manner. The impact on IT short-range plans is considered if the IT long-range plan alters.
2. The change process allows for review should specific individual events occur that may impact the validity of the IT long-range plan, and for the periodic review of the validity of the plan with regard to current business goals, processes and risks; the monitoring of defined performance indicators; and potential opportunities provided by technological evolution as identified through regular analysis of industry trends.
3. When modification is required to IT long-range plans, formal review and acceptance steps are followed, which may include input from stakeholders, a risk assessment process and the redefinition of performance indicators.
4. The IT long-range plan is regularly updated with results from organisationwide risk reviews including business, environmental, technology and human resources assessments. When risk ratings change, IT long-range planners are informed and consideration is given as to whether to amend the plan accordingly.

PO1.5 Short-range Planning for the IT Function

Why Do It?

Short-range planning within the IT function will:
- Support the achievement of the IT long-range plan by the definition of specific short-range targets that have given consideration to the resources available to the IT function
- Contribute to the monitoring and evaluation of the IT long-range plan through the analysis of performance and resource requirements against defined targets

Control Practices

1. A process exists whereby agreed IT long-range plans are translated in a timely manner into IT short-range operational plans, spanning a period defined by the requirements of the plans and including identification of IT resources and facilities.
2. Performance indicators, goals and risk assessment results are explicitly stated within the IT short-range plans. The objectives of the IT short-range plans are specific, measurable, accurate, relevant and timely, with clearly defined milestones and deliverables.
3. Formal and comprehensive periodic review and change management processes exist to ensure that IT short-range plans remain aligned with changes to the organisation's mission and objectives and the IT long-range plan.
4. Feasibility studies are performed early in the life span of an IT short-range plan to confirm the plan's likelihood of meeting expectations and delivering the objectives required to realise the IT long-range plan.

PO1.6 Communication of IT Plans

Why Do It?

Communication of IT plans within the organisation will:
- Create an effective mechanism for achieving buy-in from key stakeholders with regard to costs, resources and projects
- Strengthen the alignment of the IT and business functions
- Minimise the risk that IT's intended plans are not consistent with the organisation's expectations or requirements
- Support the achievement of IT and the organisation's goals by ensuring that IT staff work to a clear and understood mission

Figure 23—Control Practices for *Define a Strategic Information Technology Plan (cont.)*

Control Practices

1. A process is established for identifying stakeholders within the organisation who need to be aware of IT long- and short-range plans. Consideration is given, but not limited, to executive management; organisation strategists; business process owners; IT system and infrastructure owners; data owners; finance managers; human resource managers; and risk, compliance and audit teams.
2. A strategy for the effective communication of IT plans exists that identifies the most appropriate mechanism for each stakeholder. Methods include, but are not limited to, meetings, workshops, publication on organisational information sources (e.g., intranet) and departmental conferences.
3. A process is established to respond to feedback on the content of the IT plans. This process assesses the nature of the feedback and identifies where changes to the processes may be required for establishing the plans.

PO1.7 Monitoring and Evaluating of IT Plans

Why Do It?

The monitoring and evaluating of IT plans will:

- Confirm that the IT long- and short-range plans remain aligned with, and are contributing to, the attainment of the organisation's mission and goals
- Allow events potentially impacting the organisation's long-range plan to be evaluated and, where agreed, reflected in amendments to the IT long- and short-range plans
- Identify deviations from the IT long- and short-range plans, enabling management to take appropriate remedial action
- Allow assumptions upon which IT long- and short-range plans are based to be validated and changed, where appropriate

Control Practices

1. A process exists for the periodic gathering, documenting, prioritising and communicating of feedback on the IT long- and short-range plans. This includes input from IT, organisation management and key stakeholders. Reviews are defined with regard to the achievement of agreed targets within short-range plans, ongoing management of business risks as they relate to the plan, and quantifiable discernible improvements to business processes (e.g., costs, efficiency) and value from IT investment.
2. A process exists within which proposed amendments to IT plans, based upon the results of evaluation, are assessed and agreed.
3. A mechanism exists for feeding process improvement points back into the IT long- and short-range planning process.

PO1.8 Assessment of Existing Systems

Why Do It?

The assessment of existing systems will:

- Support the development of a current state analysis, identifying opportunities, vulnerabilities and barriers with regard to the IT infrastructure, which will provide a realistic context in which to define performance indictors within the planning process
- Enable the consideration of opportunities available within the technological market

Control Practices

1. A structured and comprehensive process exists for assessing the current state of existing IT systems and capabilities resulting in an inventory of technological solutions and current infrastructure. The focus of the assessment is against the requirements of the IT long- and short-range plans. Consideration includes, but is not limited to, strengths and weaknesses, degree of business automation, stability, complexity, development requirements, support and maintenance requirements, costs and external parties' input (including business partners and vendors).
2. A gap analysis is periodically performed comparing IT's current state against the requirements of the IT long- and short-range plans. The outcome of the evaluation includes, but is not restricted to, current requirements, current delivery to requirements, barriers to delivery of requirements, and the steps and costs required to remove restrictions.
3. Benchmarking against well-understood and reliable industry norms is an integral component of the assessment of existing systems and capabilities.

Figure 24—Audit Guidelines for *Define a Strategic Information Technology Plan*

PO1 DEFINE A STRATEGIC INFORMATION TECHNOLOGY PLAN

CONTROL OBJECTIVES	
1	IT as part of the organisation's long- and short-range plan
2	IT long-range plan
3	IT long-range planning—approach and structure
4	IT long-range plan changes
5	Short-range planning for the IT function
6	Communication of IT plans
7	Monitoring and evaluating of IT plans
8	Assessment of existing systems

BOTH HIGH-LEVEL AND DETAILED CONTROL OBJECTIVES ARE AUDITED BY:

Obtaining an understanding by:

► **Interviewing:**

Chief executive officer
Chief operations officer
Chief financial officer
Chief information officer
IT planning/steering committee members
IT senior management and human services staff

► **Obtaining:**

Policies and procedures relating to the planning process
Senior management steering roles and responsibilities
Organisation objectives and long- and short-range plans
IT objectives and long- and short-range plans
Status reports and minutes of planning/steering committee meetings

Evaluating the controls by:

► **Considering whether:**

IT or business enterprise policies and procedures address a structured planning approach
A methodology is in place to formulate and modify the plans, and at a minimum, they cover:

- Organisation mission and goals
- IT initiatives to support the organisation mission and goals
- Opportunities for IT initiatives
- Feasibility studies of IT initiatives
- Risk assessments of IT initiatives
- Optimal investment of current and future IT investments
- Reengineering of IT initiatives to reflect changes in the enterprise's mission and goals
- Evaluation of the alternative strategies for data applications, technology and organisation

Figure 24—Audit Guidelines for *Define a Strategic Information Technology Plan (cont.)*

Organisational changes, technology evolution, regulatory requirements, business process reengineering, staffing, in- and outsourcing, etc., are taken into account and adequately addressed in the planning process

Long- and short-range IT plans exist, are current and adequately address the overall enterprise, its mission and key business functions

IT projects are supported by the appropriate documentation as identified in the IT planning methodology

Checkpoints exist to ensure that IT objectives and long- and short-range plans continue to meet organisational objectives and long- and short-range plans

Review of and sign-off on IT plan by process owners and senior management occur

The IT plan assesses the existing information systems in terms of degree of business automation, functionality, stability, complexity, costs, strengths and weaknesses

The absence of long-range planning for information systems and supporting infrastructure results in systems that do not support enterprise objectives and business processes, or do not provide appropriate integrity, security and control

Assessing the compliance by:

► **Testing that:**

Minutes from IT planning/steering committee meetings reflect the planning process

Planning methodology deliverables exist and are as prescribed

Relevant IT initiatives are included in the IT long- and short- range plans (i.e., hardware changes, capacity planning, information architecture, new system development or procurement, disaster recovery planning, installation of new processing platforms, etc.)

IT initiatives support the long- and short-range plans and consider requirements for research, training, staffing, facilities, hardware and software

Technical implications of IT initiatives have been identified

Consideration has been given to optimising current and future IT investments

IT long- and short-range plans are consistent with the organisation's long- and short-range plans and organisation requirements

Plans have been changed to reflect changing conditions

IT long-range plans are periodically translated into short-range plans

Tasks exist to implement the plans

Figure 24—Audit Guidelines for *Define a Strategic Information Technology Plan (cont.)*

Substantiating the risk of control objectives not being met by:

► **Performing:**

Benchmarking of strategic IT plans against similar organisations or appropriate international standards/recognised industry best practices

A detailed review of the IT plans to ensure that IT initiatives reflect the organisation's mission and goals

A detailed review of the IT plans to determine if known areas of weakness within the organisation are being identified for improvement as part of the IT solutions contained in the plans

► **Identifying:**

IT failures to meet the organisation's missions and goals

IT failures to match short-range plans with long-range plans

IT project failures to meet short-range plans

IT failures to meet cost and time guidelines

Missed business opportunities

Missed IT opportunities

Figure 25—Management Guidelines for *Define a Strategic Information Technology Plan*

PO1 Plan and Organise

Define a Strategic Information Technology Plan

Control over the IT process ***define a strategic IT plan*** with the business goal of striking an optimum balance of information technology opportunities and IT business requirements as well as ensuring its further accomplishment

ensures delivery of information to the business that addresses the required information criteria and is measured by key goal indicators

is enabled by a strategic planning process undertaken at regular intervals giving rise to long-term plans; the long-term plans should periodically be translated into operational plans setting clear and concrete short-term goals

considers critical success factors that leverage specific IT resources and is measured by key performance indicators

Information Criteria	
P	Effectiveness
S	Efficiency
	Confidentiality
	Integrity
	Availability
	Compliance
	Reliability

(**P**) primary (**S**) secondary

IT Resources	
✓	People
✓	Applications
✓	Technology
✓	Facilities
✓	Data

(✓) applicable to

Critical Success Factors

- The planning process provides for a prioritisation scheme for the business objectives and quantifies, where possible, the business requirements.
- Management buy-in and support are enabled by a documented methodology for the IT strategy development, the support of validated data and a structured, transparent decision-making process.
- The IT strategic plan clearly states a risk position, such as leading-edge or road-tested, innovator or follower, and the required balance between time-to-market, cost of ownership and service quality.
- All assumptions of the strategic plan have been challenged and tested.
- The processes, services and functions needed for the outcome are defined, but are flexible and changeable with a transparent change control process.
- A reality check of the strategy by a third party has been conducted to increase objectivity and is repeated at appropriate times.
- IT strategic planning is translated into road maps and migration strategies.

Key Goal Indicators

- Percent of IT and business strategic plans that are aligned and cascaded into long- and short-range plans leading to individual responsibilities
- Percent of business units that have clear, understood and current IT capabilities
- Management survey that determines clear link between responsibilities and the business and IT strategic goals
- Percent of business units using strategic technology covered in the IT strategic plan
- Percent of IT budget championed by business owners
- Acceptable and reasonable number of outstanding IT projects

Key Performance Indicators

- Currency of IT capabilities assessment (number of months since last update)
- Age of IT strategic plan (number of months since last update)
- Percent of participant satisfaction with the IT strategic planning process
- Time lag between change in the IT strategic plans and changes to operating plans
- Index of participants involved in strategic IT plan development, based on size of effort, ratio of involvement of business owners to IT staff and number of key participants
- Index of quality of the plan, including timelines of development effort, adherence to structured approach and completeness of plan

Figure 25—Management Guidelines for *Define a Strategic Information Technology Plan (cont.)*

PO1 Maturity Model

Control over the IT process ***define a strategic IT plan*** with the business goal of striking an optimum balance of information technology opportunities and IT business requirements as well as ensuring its further accomplishment

0 **Nonexistent**—IT strategic planning is not performed. There is no management awareness that IT strategic planning is needed to support business goals.

1 **Initial/*Ad Hoc***—The need for IT strategic planning is known by IT management, but there is no structured decision process in place. IT strategic planning is performed on an as-needed basis in response to a specific business requirement and results are therefore sporadic and inconsistent. IT strategic planning is occasionally discussed at IT management meetings, but not at business management meetings. The alignment of business requirements, applications and technology takes place reactively, driven by vendor offerings, rather than by an organisationwide strategy. The strategic risk position is identified informally on a project-by-project basis.

2 **Repeatable but Intuitive**—IT strategic planning is understood by IT management, but is not documented. IT strategic planning is performed by IT management, but shared with business management only on an as-needed basis. Updating of the IT strategic plan occurs only in response to requests by management and there is no proactive process for identifying those IT and business developments that require updates to the plan. Strategic decisions are driven on a project-by-project basis, without consistency with an overall organisation strategy. The risks and user benefits of major strategic decisions are being recognised, but their definition is intuitive.

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

4 **Managed and Measurable**—IT strategic planning is standard practice and exceptions would be noticed by management. IT strategic planning is a defined management function with senior-level responsibilities. With respect to the IT strategic planning process, management is able to monitor it, make informed decisions based on it and measure its effectiveness. Both short-range and long-range IT planning occurs and is cascaded down into the organisation, with updates done as needed. The IT strategy and organisationwide strategy are increasingly becoming coordinated by addressing business processes and value-added capabilities and by leveraging the use of applications and technologies through business process reengineering. There is a well-defined process for balancing the internal and external resources required in system development and operations. Benchmarking against industry norms and competitors is becoming increasingly formalised.

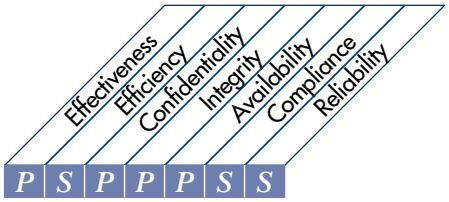
5 **Optimised**—IT strategic planning is a documented, living process, is continuously considered in business goal setting and results in discernible business value through investments in IT. Risk and value-added considerations are continuously updated in the IT strategic planning process. There is an IT strategic planning function that is integral to the business planning function. Realistic long-range IT plans are developed and constantly updated to reflect changing technology and business-related developments. Short-range IT plans contain project task milestones and deliverables, which are continuously monitored and updated as changes occur. Benchmarking against well-understood and reliable industry norms is a well-defined process and is integrated with the strategy formulation process. The IT organisation identifies and leverages new technology developments to drive the creation of new business capabilities and improve the competitive advantage of the organisation.

Figure 26—Control Objectives for *Define a Strategic Information Technology Plan*

HIGH-LEVEL CONTROL OBJECTIVE

PO9 Plan and Organise

Assess Risks



Control over the IT process of

assessing risks

that satisfies the business requirement

of supporting management decisions through achieving IT objectives and responding to threats by reducing complexity, increasing objectivity and identifying important decision factors

is enabled by

the organisation engaging itself in IT risk identification and impact analysis, involving multidisciplinary functions and taking cost-effective measures to mitigate risks

and takes into consideration

- Risk management ownership and accountability
- Different kinds of IT risks (technology, security, continuity, regulatory, etc.)
- Defined and communicated risk tolerance profile
- Root cause analyses and risk brainstorming sessions
- Quantitative and/or qualitative risk measurement
- Risk assessment methodology
- Risk action plan
- Timely reassessment

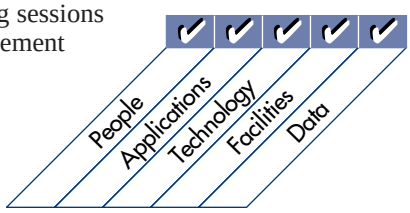


Figure 26—Control Objectives for *Define a Strategic Information Technology Plan (cont.)*

DETAILED CONTROL OBJECTIVES

9 ASSESS RISKS

9.1 Business Risk Assessment

CONTROL OBJECTIVE

Management should establish a systematic risk assessment framework. Such a framework should incorporate a regular assessment of the relevant information risks to the achievement of the business objectives, forming a basis for determining how the risks should be managed to an acceptable level. The process should provide for risk assessments at both the global level and system-specific level, for new projects as well as on a recurring basis, and with cross-disciplinary participation. Management should ensure that reassessments occur and that risk assessment information is updated with results of audits, inspections and identified incidents.

9.2 Risk Assessment Approach

CONTROL OBJECTIVE

Management should establish a general risk assessment approach that defines the scope and boundaries, the methodology to be adopted for risk assessments, the responsibilities and the required skills. Management should lead the identification of the risk mitigation solution and be involved in identifying vulnerabilities. Security specialists should lead threat identification, and IT specialists should drive the control selection. The quality of the risk assessments should be ensured by a structured method and skilled risk assessors.

9.3 Risk Identification

CONTROL OBJECTIVE

The risk assessment approach should focus on the examination of the essential elements of risk and the cause/effect relationship between them. The essential elements of risk include tangible and intangible assets, asset value, threats, vulnerabilities, safeguards, consequences and likelihood of threat. The risk identification process should include qualitative and, where appropriate, quantitative risk ranking and should obtain input from management brainstorming, strategic planning, past audits and other assessments. The risk assessment should consider business, regulatory, legal, technology, trading partner and human resources risks.

9.4 Risk Measurement

CONTROL OBJECTIVE

The risk assessment approach should ensure that the analysis of risk identification information results in a quantitative and/or qualitative measurement of risk to which the examined area is exposed. The risk acceptance capacity of the organisation should also be assessed.

9.5 Risk Action Plan

CONTROL OBJECTIVE

The risk assessment approach should provide for the definition of a risk action plan to ensure that cost-effective controls and security measures mitigate exposure to risks on a continuing basis. The risk action plan should identify the risk strategy in terms of risk avoidance, mitigation or acceptance.

9.6 Risk Acceptance

CONTROL OBJECTIVE

The risk assessment approach should ensure the formal acceptance of the residual risk, depending on risk identification and measurement, organisational policy, uncertainty incorporated in the risk assessment approach itself, and the cost-effectiveness of implementing safeguards and controls. The residual risk should be offset with adequate insurance coverage, contractually negotiated liabilities and self-insurance.

continued on next page

Figure 26—Control Objectives for *Define a Strategic Information Technology Plan (cont.)*

9.7 **Safeguard Selection**
CONTROL OBJECTIVE
While aiming for a reasonable, appropriate and proportional system of controls and safeguards, controls with the highest return on investment (ROI) and those that provide quick wins should receive first priority. The control system also should balance prevention, detection, correction and recovery measures. Furthermore, management should communicate the purpose of the control measures, manage conflicting measures and monitor the continuing effectiveness of all control measures.

9.8 **Risk Assessment Commitment**
CONTROL OBJECTIVE
Management should encourage risk assessment as an important tool in providing information in the design and implementation of internal controls, in the definition of the IT strategic plan and in the monitoring and evaluation mechanisms.

Figure 27—Control Practices for *Assess Risks*

PO9.1 Business Risk Assessment

Why Do It?
The provision of a systematic risk assessment framework in line with control practices will:
- Avoid a decline in the effectiveness of the risk assessment process over time as a result of staff turnover and the time taken to transfer knowledge between skilled risk assessors and new recruits
- Ensure frequent updates to accommodate new forms of business and IT risk (e.g., the loss of intellectual capital, which weakens the capability for business innovation)
- Promote the effective management of risk
- Result in opportunities for organisational synergy and avoidance of duplication of risk management effort by aligning the IT risk assessment framework with the broader corporate and IT governance processes
- Involve senior management representing the major business and IT functions and, therefore, increase the initial acceptance of the framework and facilitate the continued and active support of the risk assessment process

Control Practices
1. Senior management representing the major business and IT functions develops a systematic risk assessment framework and establishes a policy to define risk limits and risk tolerance.
2. An integrated business and IT risk assessment framework and approach, which forms part of the broader corporate governance initiatives, are used. This integrated framework supports a holistic risk assessment approach that reviews the global as well as systems-specific risk.
3. The business risk assessment process is regularly updated with the results of audits, inspections and identified incidents. The potential business impact of new technologies is continually evaluated and is also used to update the risk assessment process.
4. The risk assessment framework provides an important input to both the business and the IT strategy. The value of this input is increased by the participation of senior management from across the organisation in the risk assessment process and the continual scanning of new technologies that impact the business.

PO9.2 Risk Assessment Approach

Why Do It?
Establishing a risk assessment approach along the lines of the control practices will:
- Allow appropriate planning of required skills and resources to build risk assessment teams that have organisational credibility
- Ensure that the risk assessment approach or strategy will stand up to best practice experience from other businesses in the industry or similar organisations
- Facilitate the acceptance and implementation of recommendations by key stakeholders
- Increase the degree of internalising the risk assessment framework in the thinking and actions of staff to ensure their active support of the programme
- Maximise the value-added potential of the risk management function

Control Practices
1. The need to prepare and maintain a systematic risk assessment process is defined in a policy.
2. The clear and unambiguous statement of management direction improves the general level of understanding of the risk assessment framework and process.
3. The business risk assessment process is clearly and routinely communicated to the entire organisation. Communication improves awareness of the business risk and the knowledge of what to do to reduce risk.
4. Management establishes a general risk assessment approach, which defines the scope, boundaries and the methodology to be adopted for risk assessments.
5. Individual accountability for risk management is assigned and accepted and performance is monitored.
6. The responsibility for the preparation, maintenance and approval of business risk assessment plans is identified, and the required skills for this task are available within the organisation. Senior management from across the organisation is involved.
7. The required skills and resources required to perform risk assessments are clearly defined, agreed with by key stakeholders and made available.
8. The clear definition of the expected outputs of the risk assessment process are agreed by stakeholders.
9. Cross-functional teams apply the risk assessment approach. Depending on the nature of the assignment, these teams are comprised of representatives from IS/IT, risk management and business groups. The members of the risk assessment work group are trained in the risk management process.
10. Skilled risk assessors regularly apply a structured method for reviewing both the effectiveness and efficiency of the risk assessment process. Process improvement recommendations and gaps or weaknesses in risk assessments are communicated to the assessment teams.
11. The risk assessment process is business process-driven, with business managers responsible for certain parts of risk assessment. This is done to improve business and IT alignment, focus controls or countermeasures, and make the overall risk assessment approach more cost-effective.

Figure 27—Control Practices for *Assess Risks (cont.)*

12. The risk assessment approach, although structured and rigorous in design, supports customised implementations that are based on specific risk review requirements. The flexibility of the risk assessment approach enables the review team to select the approach best suited to the various types of IT risks (e.g., technology and continuity).
13. The risk assessment process forms a pervasive part of the systems and application software life cycles.
14. A reality check of the strategy is conducted by a third party to increase objectivity and is repeated at appropriate times. Where possible, information is exchanged with peer groups to validate the approach.

PO9.3 Risk Identification

Why Do It?
Risk identification performed in line with the control practices will:
- Ensure that all risks and events that can trigger other risks are identified and included in further analysis
- Ensure that the risk mitigation efforts are correctly categorised and prioritised
- Enable the performance of continuous risk identification throughout the life of projects and systems and application software life cycles

Control Practices
1. The existing management, technical systems and procedures are identified to control risk and assess their strengths and weaknesses using checklists, judgements based on experience and records, flow charts, brainstorming, systems analysis and engineering, and scenario analysis.
2. The project is separated into a set of elements that provides a logical framework to help ensure that significant risks are not overlooked. A comprehensive list of events that might affect each element of the project is generated.
3. For each risk event, a comprehensive list of causes, scenarios, consequences and interrelationships is developed.
4. A baseline set of risks is established early in the project.

PO9.4 Risk Measurement

Why Do It?
Risk measurement in line with the control practices will:
- Ensure that only unique, relevant risks are considered for detailed analysis
- Ensure precise estimates of the cost of risk mitigation
- Ensure that relationships amongst risks are identified
- Maximise the number of risk mitigation options available to management

Control Practices
1. Risks are evaluated 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. Risks are classified based on their shared characteristics.
3. Risks are prioritised 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, pare to top "N" and top five.
4. The likelihood of occurrence of each major risk to be studied is qualified. Likelihood may be determined using statistical analysis and probability determinations based on reasonable sources of information that can be appropriately validated. Confidence intervals are estimated for the levels of risk to allow performance of sensitivity analysis on the estimated level of risk. A sensitivity analysis is conducted on the results of the quantitative analysis to test the effect of changes in the assumptions and data.
5. The risk acceptance capacity of the organisation is assessed by comparing risks and their mitigation costs.

PO9.5 Risk Action Plan

Why Do It?
Risk action plans in line with the control practices will:
- Provide a means for management to determine whether the effectiveness of existing controls (i.e., policies, procedures or physical changes) outweighs the relative benefits of new controls
- Allow management to determine whether the adverse impact of risks is made as low as reasonably possible
- Ensure that new controls consider cost-effectiveness and relative benefits in light of the effectiveness of existing controls
- Facilitate the successful implementation of the risk mitigation controls
- Provide a framework for implementation that specifies the methods chosen, assigns responsibilities and individual accountabilities for actions, and monitors them against criteria specified by management

Control Practices
1. Using the risk inventory and priorities, options/countermeasures are identified to mitigate risk, including avoiding risk, reducing the likelihood of occurrence, reducing the consequences and transferring the risk (i.e., sharing risk with another party/organisation).

Figure 27—Control Practices for *Assess Risks (cont.)*

2. The benefits and costs of applying risk mitigation options/countermeasures (controls) individually or in combination are determined.
3. The cost of implementing each option is balanced against the benefits derived from it. The impact identified in the first control practice in PO9.4 is considered and the effect of uneconomic events on the decision are also considered.
4. The risk mitigation controls to be included in the risk action plan are selected.
5. The risk action plan on implementing the chosen risk mitigation controls is documented. Responsibilities, schedules, expected outcome of risk mitigation (including residual risk), budgeting, performance measures and the review process to be set in place are identified.

PO9.6 Risk Acceptance

Why Do It?
Risk acceptance, when organised considering the control practices, will ensure that:
- Management is aware of the global residual business risk that is not covered by the internal control system or insurance.
- The impact and probability of risks transferred to third parties are known and used to validate the premiums for coverage and adequacy of the coverage.

Control Practices
1. If, after implementation of the risk mitigation option/countermeasure, there is still residual risk, a decision is made whether to retain the risk, negotiate contractual liabilities or repeat the risk mitigation option/countermeasure.
2. When the risk is retained, it is either formally recognised as an accepted business risk (potentially mitigated by self-insurance) or transferred to a third party (typically an insurer). If risks are transferred, management ensures that the appropriate balance between premium and compensation is maintained (taking into account the probability and impact of such risks).

PO9.7 Safeguard Selection

Why Do It?
Safeguards selected considering the control practices will:
- Be economically justifiable
- Take into account how risk is perceived
- Appropriately communicate to those who need to know inside and outside the organisation
- Be part of a set that effectively and efficiently protects the organisation's assets

Control Practices
1. Safeguard options are assessed considering the extent of risk reduction and the extent of additional benefits/opportunities created. The options to treat risk are in line with the way risk is perceived in the organisation.
2. Cost-benefit analysis is performed for safeguard options, taking into account that the best economic solution may still require transferring risk or implementing supplementary controls.
3. When the cost of selected safeguard options exceeds the available budget, safeguard options are prioritised.
4. The most appropriate way to inform affected parties of the selected risk treatment options is determined.
5. A process is implemented to ensure reviews of the chosen safeguards for their continued efficiency and effectiveness to protect the integrity, confidentiality and availability of the organisation's assets.

PO9.8 Risk Assessment Commitment

Why Do It?
Commitment to risk assessment as suggested in the control practices will:
- Promote a risk management mentality in the organisation
- Encourage line management and staff to actively provide input in the research, implementation and assessment of mitigating controls
- Ensure that input from risk management is considered a mandatory input for the IT strategy and the internal control framework

Control Practices
1. A sponsor and champion for risk management are appointed at the executive level.
2. An organisational unit, such as a specialist risk management function, is established that has enterprisewide responsibility for promoting good practice in risk management.
3. Direct access to all levels of management throughout the organisation is provided to the manager of the risk management function, who is required to maintain contact with peers in the commercial world, counterparts in government, law enforcement agencies and external risk management specialists.

Figure 28—Audit Guidelines for *Assess Risks*

PO9 ASSESS RISKS

CONTROL OBJECTIVES	
1	Business risk assessment
2	Risk assessment approach
3	Risk identification
4	Risk measurement
5	Risk action plan
6	Risk acceptance
7	Safeguard selection
8	Risk assessment commitment

BOTH HIGH-LEVEL AND DETAILED CONTROL OBJECTIVES ARE AUDITED BY:

Obtaining an understanding by:

► **Interviewing:**

Senior management of the IT function
Selected IT staff
Selected risk management personnel
Key users of IT services

► **Obtaining:**

Policies and procedures relating to risk assessment
Business risk assessment documents
Operating risk assessment documents
IT risk assessment documents
Details of the basis upon which risk and exposure to risk are measured
Personnel files for selected risk assessment personnel
Insurance policies covering residual risk
Results of expert opinions
Peer group reviews
Insight from the risk management database

Evaluating the controls by:

► **Considering whether:**

Systematic risk assessment framework is in place, incorporating the relevant information risks to the achievement of the organisation's objectives and forming a basis for determining how the risks should be managed to an acceptable level
Risk assessment approach provides for regularly updated risk assessments at both the global and system-specific levels
Risk assessment procedures are in place to determine that identified risks include both external and internal factors, and take into consideration results of audits, inspections and identified incidents

Figure 28—Audit Guidelines for *Assess Risks (cont.)*

Organisationwide objectives are included in the risk identification process

Procedures for monitoring changes in systems processing activity determine that system risks and exposures are adjusted in a timely manner

Procedures exist for ongoing monitoring and improvement of the risk assessment and mitigating controls creation processes

The risk assessment documentation includes:

- A description of the risk assessment methodology
- The identification of significant exposures and the corresponding risks
- The risks and corresponding exposures that are addressed

Probability, frequency and threat analysis techniques are included in the identification of risks

Qualifications of risk assessment staff are adequate

A formal quantitative and/or qualitative (or combined) approach exists for identifying and measuring risks, threats and exposures

Calculations and other methods are used in the measurement of risks, threats and exposures

The risk action plan is used in implementing appropriate measures to mitigate risks, threats and exposures

Acceptance of residual risk takes into account:

- Organisational policy
- Risk identification and measurement
- Uncertainty incorporated in the risk assessment approach itself
- Cost and effectiveness of implementing safeguards and controls

Insurance coverage offsets the residual risk

Formal quantitative and/or qualitative approaches exist to select control measures that maximise return on investment

There is a balance between the detection, prevention, correction and recovery measures used

Formal procedures exist to communicate the purpose of the control measures

Assessing the compliance by:

► **Testing that:**

Risk assessment framework is complied with in that the risk assessments are regularly updated to reduce the risk to an acceptable level

Risk assessment documentation complies with the risk assessment framework and documentation is appropriately prepared and maintained

IT management and staff are aware of and involved in the risk assessment process

Management understands risk-related factors and threat likelihood

Relevant personnel understand and formally accept residual risk

Reports issued to senior management for review and concurrence of identified risks and use in monitoring of risk-reduction activities are timely

The approach used to analyse risk results in a quantitative or qualitative (or combined) measurement of exposure to risk

Risks, threats and exposures identified by management and risk-related attributes are used to detect each occurrence of a specific threat

The risk action plan is current and includes cost-effective controls and security measures to mitigate risk exposure

Figure 28—Audit Guidelines for *Assess Risks (cont.)*

Priorities from highest to lowest exist and, for each risk, an appropriate response exists:
- Planned preventive mitigating control
- Secondary detective control
- Tertiary corrective control

Scenarios of risk vs. control are documented, current and communicated to appropriate staff

Sufficient insurance coverage exists with respect to accepted residual risk and considered against various threat scenarios, including:
- Fire, flood, earthquake, tornadoes, terrorism and other unforeseeable disasters
- Breach of employee fiduciary responsibilities
- Business interruption—lost revenues, lost customers, etc.
- Other risks not generally covered by above IT and business risk/continuity plans

Substantiating the risk of control objectives not being met by:

► **Performing:**

Benchmarking of the risk assessment framework against similar organisations or appropriate international standards/recognised industry best practices

A detailed review of the risk assessment approach used to identify, measure and mitigate risk to an acceptable level of residual risk

► **Identifying:**

Risks not being identified

Risks not being measured

Risks not being addressed/managed to an acceptable level

Out-of-date risk assessments and/or out-of-date information in risk assessments

Faulty quantitative and/or qualitative measures of risks, threats and exposures

Risk action plans that do not provide for cost-effective controls and security measures

The lack of formal acceptance of the residual risk

Inadequate insurance coverage

Figure 29—Management Guidelines for *Assess Risks*

PO9 Plan and Organise
Assess Risks

Control over the IT process ***assess risks*** with the business goal of supporting management decisions in achieving IT objectives and responding to threats by reducing complexity, increasing objectivity and identifying important decision factors

ensures delivery of information to the business that addresses the required information criteria and is measured by key goal indicators

is enabled by the organisation engaging itself in IT risk identification and impact analysis, involving multidisciplinary functions and taking cost-effective measures to mitigate risks

considers critical success factors that leverage specific IT resources and is measured by key performance indicators

Information Criteria	
P	Effectiveness
S	Efficiency
P	Confidentiality
P	Integrity
P	Availability
S	Compliance
S	Reliability

(**P**) primary (**S**) secondary

IT Resources	
✓	People
✓	Applications
✓	Technology
✓	Facilities
✓	Data

(✓) applicable to

Key Goal Indicators

- Increased degree of awareness of the need for risk assessments
- Decreased number of incidents caused by risks identified after the fact
- Increased number of identified risks that have been sufficiently mitigated
- Increased number of IT processes that have formal, documented risk assessments completed
- Appropriate percent or number of cost-effective risk assessment measures

Critical Success Factors

- There are clearly defined roles and responsibilities for risk management ownership and management accountability.
- A policy is established to define risk limits and risk tolerance.
- The risk assessment is performed by matching vulnerabilities, threats and the value of data.
- Structured risk information is maintained, fed by incident reporting.
- Responsibilities and procedures for defining, agreeing on and funding risk management improvements exist.
- Focus of the assessment is primarily on real threats and less on theoretical ones.
- Brainstorming sessions and root cause analyses leading to risk identification and mitigation are routinely performed.
- A reality check of the strategy is conducted by a third party to increase objectivity and is repeated at appropriate times.

Key Performance Indicators

- Number of risk management meetings and workshops
- Number of risk management improvement projects
- Number of improvements to the risk assessment process
- Level of funding allocated to risk management projects
- Number and frequency of updates to published risk limits and policies
- Number and frequency of risk monitoring reports
- Number of personnel trained in risk management methodology

Figure 29—Management Guidelines for *Assess Risks (cont.)*

PO9 Maturity Model

Control over the IT process ***assess risks*** with the business goal of supporting management decisions in achieving IT objectives and responding to threats by reducing complexity, increasing objectivity and identifying important decision factors

0 **Nonexistent**—Risk assessment for processes and business decisions does not occur. The organisation does not consider the business impacts associated with security vulnerabilities and development project uncertainties. Risk management has not been identified as relevant to acquiring IT solutions and delivering IT services.

1 **Initial/*Ad Hoc***—The organisation is aware of its legal and contractual responsibilities and liabilities, but considers IT risks in an *ad hoc* manner, without following defined processes or policies. Informal assessments of project risk take place as determined by each project. Risk assessments are not likely to be identified specifically within a project plan or assigned to specific managers involved in the project. IT management does not specify responsibility for risk management in job descriptions or other informal means. Specific IT-related risks such as security, availability and integrity are occasionally considered on a project-by-project basis. IT-related risks affecting day-to-day operations are infrequently discussed at management meetings. Where risks have been considered, mitigation is inconsistent.

2 **Repeatable but Intuitive**—There is an emerging understanding that IT risks are important and need to be considered. Some approach to risk assessment exists, but the process is still immature and developing. The assessment is usually at a high level and is typically applied only to major projects. The assessment of ongoing operations depends mainly on IT managers raising it as an agenda item, which often happens only when problems occur. IT management has not generally defined procedures or job descriptions dealing with risk management.

3 **Defined Process**—An organisationwide risk management policy defines when and how to conduct risk assessments. Risk assessment follows a defined process that is documented and available to all staff through training. Decisions to follow the process and receive training are left to the individual's discretion. The methodology is convincing and sound and ensures that key risks to the business are likely to be identified. Decisions to follow the process are left to individual IT managers, and there is no procedure to ensure that all projects are covered or the ongoing operation is examined for risk on a regular basis.

4 **Managed and Measurable**—The assessment of risk is a standard procedure and exceptions to following the procedure are noticed by IT management. It is likely that IT risk management is a defined management function with senior-level responsibility. The process is advanced and risk is assessed at the individual project level and also regularly assessed with regard to the overall IT operation. Management is advised on changes in the IT environment that could significantly affect the risk scenarios, such as an increased threat from the network or technical trends that affect the soundness of the IT strategy. Management is able to monitor the risk position and make informed decisions regarding the exposure it is willing to accept. Senior management and IT management have determined the levels of risk that the organisation will tolerate and have standard measures for risk/return ratios. Management budgets for operational risk management projects to reassess risks on a regular basis. A risk management database is established.

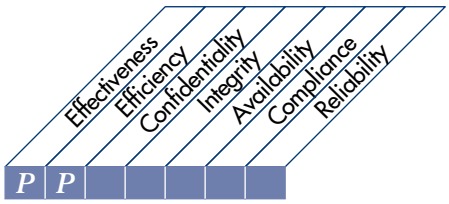
5 **Optimised**—Risk assessment has developed to the stage that a structured, organisationwide process is enforced, followed regularly and well managed. Risk brainstorming and root cause analysis, involving expert individuals, are applied across the entire organisation. The capturing, analysis and reporting of risk management data are highly automated. Guidance is drawn from leaders in the field, and the IT organisation takes part in peer groups to exchange experiences. Risk management is truly integrated into all business and IT operations, is well accepted and extensively involves the users of IT services.

Figure 30—Control Objectives for *Manage Projects*

HIGH-LEVEL CONTROL OBJECTIVE

PO10 Plan and Organise

Manage Projects



Control over the IT process of

managing projects

that satisfies the business requirement

to set priorities and to deliver on time and within budget

is enabled by

the organisation identifying and prioritising projects in line with the operational plan and the adoption and application of sound project management techniques for each project undertaken

and takes into consideration

- Business management sponsorship for projects
- Program management
- Project management capabilities
- User involvement
- Task breakdown, milestone definition and phase approvals
- Allocation of responsibilities
- Rigorous tracking of milestones and deliverables
- Cost and manpower budgets, balancing internal and external resources
- Quality assurance plans and methods
- Program and project risk assessments
- Transition from development to operations

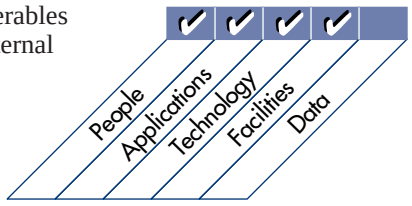


Figure 30—Control Objectives for *Manage Projects (cont.)*

DETAILED CONTROL OBJECTIVES

10 MANAGE PROJECTS

10.1 **Project Management Framework**
CONTROL OBJECTIVE
Management should establish a general project management framework that defines the scope and boundaries of managing projects, as well as the project management methodology to be adopted and applied to each project undertaken. The methodology should cover, at a minimum, the allocation of responsibilities, task breakdown, budgeting of time and resources, milestones, check points and approvals.

10.2 **User Department Participation in Project Initiation**
CONTROL OBJECTIVE
The organisation's project management framework should provide for participation by the affected user department management in the definition and authorisation of a development, implementation or modification project.

10.3 **Project Team Membership and Responsibilities**
CONTROL OBJECTIVE
The organisation's project management framework should specify the basis for assigning staff members to the project and define the responsibilities and authorities of the project team members.

10.4 **Project Definition**
CONTROL OBJECTIVE
The organisation's project management framework should provide for the creation of a clear written statement defining the nature and scope of every implementation project before work on the project begins.

10.5 **Project Approval**
CONTROL OBJECTIVE
The organisation's project management framework should ensure that for each proposed project, the organisation's senior management reviews the reports of the relevant feasibility studies as a basis for its decision on whether to proceed with the project.

10.6 **Project Phase Approval**
CONTROL OBJECTIVE
The organisation's project management framework should provide for designated managers of the user and IT functions to approve the work accomplished in each phase of the cycle before work on the next phase begins.

10.7 **Project Master Plan**
CONTROL OBJECTIVE
Management should ensure that for each approved project, a project master plan is created that is adequate for maintaining control over the project throughout its life and includes a method of monitoring the time and costs incurred throughout the life of the project. The content of the project plan should include statements of scope, objectives, required resources and responsibilities and should provide information to permit management to measure progress.

10.8 **System Quality Assurance Plan**
CONTROL OBJECTIVE
Management should ensure that the implementation of a new or modified system includes the preparation of a quality plan that is then integrated with the project master plan and formally reviewed and agreed to by all parties concerned.

continued on next page

Figure 30—Control Objectives for *Manage Projects (cont.)*

10.9 **Planning of Assurance Methods**
CONTROL OBJECTIVE
Assurance tasks should be identified during the planning phase of the project management framework. Assurance tasks should support the accreditation of new or modified systems and should assure that internal controls and security features meet the related requirements.

10.10 **Formal Project Risk Management**
CONTROL OBJECTIVE
Management should implement a formal project risk management programme for eliminating or minimising risks associated with individual projects (i.e., identifying and controlling the areas or events that have the potential to cause unwanted change).

10.11 **Test Plan**
CONTROL OBJECTIVE
The organisation's project management framework should require that a test plan be created for every development, implementation and modification project.

10.12 **Training Plan**
CONTROL OBJECTIVE
The organisation's project management framework should require that a training plan be created for every development, implementation and modification project.

10.13 **Post-implementation Review Plan**
CONTROL OBJECTIVE
The organisation's project management framework should provide for as an integral part of the project team's activities, the development of a plan for a post-implementation review of every new or modified information system to ascertain whether the project has delivered the planned benefits.

Figure 31—Control Practices for *Manage Projects*

PO10.1 Project Management Framework

Why Do It?
The establishment of a project management framework in line with control practices will:
- Increase the likelihood of project success by establishing clear, repeatable, measurable, auditable and interlinked project management activities
- Reduce the cost associated with establishing project management activities and disciplines for each new project undertaken
- Facilitate effective communication of project objectives, project management activities and project progress through a common and consistent understanding of the project management approach
- Provide a consistent approach, tools and processes supporting comparative assessments of projects across the organisation

Control Practices
1. Management establishes a project management framework to be adopted and applied to each project.
2. The project management framework is consistent with, and an integral component of, the organisation's programme management framework. The framework is subject to periodic assessment to ensure its ongoing appropriateness in light of changing conditions.
3. The project management framework establishes senior management sponsorship of projects. The project sponsor's role, responsibilities and accountabilities are clearly defined and supported by the required level of decision-making authority within the organisation. An indication of the level of involvement required to effectively fulfil the role is included in the role description.
4. The organisation performs a periodic assessment of its programme and project management capabilities against the project management framework and the organisation's portfolio of projects. Gaps in capability are identified and addressed appropriately.
5. The project management framework includes guidance on the role and use of an existing programme or project office, or the creation of such a function for a project.
6. The project management framework includes a change control process for recording, evaluating, communicating and authorising changes to the project scope, project requirements or system design.
7. The project management framework considers the requirements for controlling the organisation's portfolio of projects.
8. The project management framework satisfies local statute and regulatory requirements for project management.

PO10.2 User Department Participation in Project Initiation

Why Do It?
The involvement of key stakeholders and the user department in project initiation (and throughout the project's life cycle) in line with the control practices will:
- Increase the likelihood of the project being driven by, and delivering, business benefits
- Clarify the responsibilities and accountabilities of the business, as well as IT, in ensuring project success
- Establish a common understanding across the business, end users and IT personnel of the objectives of the project and the resources required from all parties
- Ensure increased user commitment and buy-in to the project

Control Practices
1. The project management framework provides for participation by key stakeholders, including management of the affected user department and key end users, in the initiation, definition and authorisation of a project.
2. Ongoing key stakeholder and user department participation for the remainder of the project life cycle is outlined during project initiation and further refined during 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 materials development.

PO10.3 Project Team Membership and Responsibilities

Why Do It?
The formal definition and documentation of project team membership and responsibilities in line with control practices will:
- Facilitate the appropriate staffing of the project with the required skills and resources, potentially highlighting resource shortfalls
- Reduce the risk of assumptions being made that lead to gaps or overlaps in project activities
- Avoid confusion and wasted resources through clarifying communication and reporting lines and escalation procedures
- Enable interested parties within and external to the project to more quickly identify and communicate with appropriate project team members

Figure 31—Control Practices for *Manage Projects (cont.)*

Control Practices

1. The project management framework specifies the basis for assigning staff members to projects and defines the responsibilities, accountabilities and authorities of the project team members, and project governance and support functions (e.g., project board, programme or project office, project sponsor). In particular, clear accountability exists for the delivery of business benefits.
2. Resource needs are identified for the project, and appropriate roles and responsibilities are clearly mapped out, with escalation and decision-making authorities agreed and understood.
3. Experienced project management and team leader resources, with skills appropriate to the size, complexity and risk of the project being undertaken, are utilised.
4. Responsibility for procurement and management of third-party project and system support relationships is clearly defined and agreed.
5. The roles and responsibilities of other interested parties are considered and clearly defined, including, but not limited to, internal audit, compliance, finance, legal, procurement and human resources.

PO10.4 Project Definition

Why Do It?

The establishment of a project definition in line with the control practices will:

- Provide a baseline against which the progress and, ultimately, the success of the project can be measured
- Assign and clarify accountabilities, including those of key business stakeholders
- Reduce the likelihood of misunderstood project objectives impacting staff morale, the effective use of resources and the level of commitment to the project
- Facilitate the preparation of a master project plan
- Facilitate future maintenance by ensuring availability of an adequate specification of project objectives and requirements

Control Practices

1. The project management framework provides for the creation of a clear, written statement defining the nature, scope and business benefit of every project, before work on the project begins.
2. The requirements for the project are agreed and signed off by key stakeholders within the organisation and IT, including initial consideration of high-level critical success factors and key performance indicators. The approved document is accessible to key stakeholders in read-only mode.
3. A formal systems development life cycle (SDLC) approach is defined, appropriate to the objectives of the project. The approach specifies the development phases required and the standards, policies and procedures appropriate to each. Planned variances from the full SDLC approach are noted and explained in the project definition.
4. Nonfunctional requirements (e.g., security, backup and contingency, system performance, data migration) are considered within the project definition unless an alternative suitable milestone for their subsequent consideration is established.
5. The project definition outlines the requirements for a project stakeholder analysis and communication plan that identifies to whom communication needs to be made within and outside of the project, and the most effective means of doing so. The communication plan is maintained throughout the project, reflecting the changing needs as the project moves from initiation to implementation.

PO10.5 Project Approval

Why Do It?

Defining and executing a project approval process in line with the control practices will:

- Ensure that projects are based on criteria aligned to the organisation's vision
- Increase key stakeholder and end-user commitment to the project, or identify at an early stage if there is a lack of commitment to the project's objectives
- Provide senior management with the opportunity to question the preferred approach and gain confidence that alternative solutions have been considered and the most appropriate are selected
- Help ensure that only projects that are prioritised are initiated

Control Practices

1. The project management framework ensures that for each proposed project the organisation's senior management reviews the reports of the relevant feasibility studies to confirm the nature of the project justification (e.g., nondiscretionary, financial, strategic or discretionary) and its fit with organisational priorities, and establishes a basis for making a decision on whether to proceed with the project.
2. Alternative solutions to satisfying the organisation's requirements and supporting and maintaining the solution and its associated business processes (e.g., internally or externally) are identified and evaluated.
3. A feasibility study of the preferred approach includes high-level definition of the project's business case, including an assessment of development costs, operational costs (business and IT), business benefit realisation, payback period and risks to the project and existing systems. The project's business case is further refined in subsequent project phases as more detail becomes available.

Figure 31—Control Practices for *Manage Projects (cont.)*

4. Key stakeholders formally sign a project approval document that is filed and subject to rigorous document version control.

PO10.6 Project Phase Approval

Why Do It?
Defining and performing project phase approvals in line with the control practices will:
- Enable overall progress on project delivery and benefit realisation to be reassessed and mitigating actions to be taken where variances arise, including timely consideration of early project termination
- Reduce the risk of scope creep occurring through formal and regular management consideration of project and project phase critical success factors
- Maintain key stakeholder and end-user commitment and accountability for the project
- Provide concrete evidence of progress to project team and end users, formally recognising their efforts to that point
- Ensure that each phase of the project is in conformity with the project definition

Control Practices
1. The project management framework provides for designated managers and end users of the affected business and IT functions to approve and sign off on the deliverables produced in each project phase (e.g., requirements analysis, design, build, test, go-live) of the systems development life cycle, before work on the next phase begins.
2. The approval process is based on clearly defined acceptance criteria agreed by key stakeholders prior to work commencing on the project phase deliverable and, at a minimum, in advance of the completion of the deliverables for a phase.
3. The approval process includes consideration of actual costs for the phase vs. budgeted and projected costs. Significant variances are assessed against the project's expected benefits, approved by the appropriate project governance function (e.g., project board, project sponsor) and reflected in the project's business case.
4. The project phase acceptance criteria to consider, where appropriate, are the completion of supporting processes, such as delivery of operational policies and procedures, training and software tools, and more readily identifiable products, such as design documents or tested code.
5. Key stakeholders and end users formally sign a project phase approval document, which is filed and subject to rigorous document version control.
6. Prior to implementation, the readiness of the project to go live is approved through a formally conducted "stop/go" assessment based on predetermined critical success factors aimed at determining system quality and the preparedness of the business and support functions to use and maintain the system.

PO10.7 Project Master Plan

Why Do It?
Establishing a project master plan and assessing project activities and progress against it in line with the control practices will:
- Reduce the risk that project milestones are missed and the likelihood of the project failing to deliver to time, budget or scope
- Increase management's awareness of potential project slippage and the ability to react in a timely manner
- Allow initial estimating errors to be identified and addressed
- Provide a mechanism for sharing project plan and progress details in a consistent manner within and external to the project

Control Practices
1. A project plan is established for each approved project.
2. The project plan provides information to permit management to measure project progress. The project plan includes, but is not limited to, statement of scope, details of project products and deliverables, required resources and responsibilities, clear work breakdown structures and work packages, estimates of resources required, milestones, key dependencies, and identification of a critical path.
3. Checkpoint reports are produced and reviewed on a regular basis, summarising status of work against plan, and actual costs against budget. Significant variances are escalated appropriately within the project governance structure.
4. The project master plan and any dependent plans are updated, with the agreement of the plan owner, to reflect actual progress and material changes from master project plan checkpoints.

PO10.8 System Quality Assurance Plan

Why Do It?
The establishment and execution of a system quality assurance plan in line with the control practices will:
- Increase the likelihood of the implemented system or system modification meeting business and user requirements
- Reduce the risk that the implemented system or system modification will adversely impact upon existing systems and the underlying technical architecture

Figure 31—Control Practices for *Manage Projects (cont.)*

- Establish a consistent level of quality assurance activity across the project, including third parties, which can be incorporated in a timely manner to the project costs and master project plan

Control Practices

1. A quality plan, integrated with the project plan, is established and is formally reviewed and agreed by interested parties.
2. The quality plan clearly identifies metrics, responsibilities and ownership for providing quality assurance of the business solution, the application solution and the technical infrastructure solution.
3. The quality plan outlines the requirements, where appropriate, for independent validation and verification of the business and technical solution.
4. The scope of the quality plan includes project products under development by third parties.

PO10.9 Planning of Assurance Methods

Why Do It?

The planning and execution of assurance methods in line with the control practices will:

- Satisfy external requirements for assurance (e.g., external audit) in a timely and cost-effective manner
- Increase the confidence of key stakeholders internally (e.g., audit committee, project sponsor, project board, chief financial officer, chief executive officer) that the project is under control and on track to realise business benefits
- Facilitate external accreditation of systems or systems modifications

Control Practices

1. Assurance tasks are identified during the planning phase of the project management framework and incorporated into the project master plan.
2. Requirements for accreditation of systems are appropriately considered, including the need for assurance over internal control and security features.
3. The execution of a programme and/or project assurance function by appropriately skilled and experienced independent resources is incorporated into the project master plan. The programme assurance role is independent of the project and this role reports to an appropriate decision-making level (e.g., project board, project sponsor).

PO10.10 Formal Project Risk Management

Why Do It?

The formal management of project risks and issues in line with the control practices will:

- Enable the early identification of potential showstoppers when considering project feasibility and approval
- Allow management to identify and plan for contingencies and countermeasures to reduce the likelihood of project risks and issues adversely impacting the success of the project
- Assist management by enabling a focus of contingency resources on highest priority risks and issues in a cost-effective manner
- Enable risk and issue owners to be clearly identified and mitigating actions to be monitored

Control Practices

1. A formal project risk management framework is established. The consideration of risks includes an assessment of priority based on potential impact and likelihood, with mitigating resources focused on the highest priority risks.
2. Responsibility for executing the organisation's project risk management framework within a project is clearly assigned to an appropriately skilled individual. This role is either performed by the project manager or delegated by the project manager to another member of the project team.
3. Identified project risks and issues are managed and discussed at an appropriate level within the project governance structure.
4. Project risks are reassessed periodically, including at entry into each major project phase and as part of major change request assessments.
5. A project risk log and a project issues log are maintained and reviewed regularly.
6. Risk and issue owners are identified and mitigating actions and/or contingency plans are identified. Owners of actions are assigned, cost implications are considered, and actions are managed to agreed action due dates.

PO10.11 Test Plan

Why Do It?

Developing and executing a test plan in line with control practices will:

- Increase the likelihood that testing is performed in a structured, efficient, repeatable and auditable manner
- Reduce the risk that the project's products and deliverables fail to meet user functional requirements and IT operational needs

Figure 31—Control Practices for *Manage Projects (cont.)*

- Provide a baseline against which testing progress can be assessed
- Enable management information to be produced that highlights trends and specific issues to be considered by project management in assessing project progress against the project master plan
- Facilitate the setting up and running of automated test scripts

Control Practices

1. A testing strategy is considered and every project has a documented and adhered-to test plan.
2. The role of test manager is assigned, with responsibility for co-ordination across testing stages and maximising efficient use of test resources, procedures and tools. The test plan identifies and documents resources required to execute the test plan, including, but not limited to, test planners, test executors, automated testing tools, test environments and test hardware.
3. The test plan clarifies the different testing stages appropriate to the project, including, but not limited to, unit test, system test, integration test, user acceptance test, volume/stress/performance test, data conversion test and operational readiness test.
4. The test plan also includes steps to assure that subsequent project development activity does not adversely impact previously completed testing (i.e., regression testing).
5. For each test stage, the test plan includes, but is not limited to, the test stage objectives, the outline testing approach, and the entry and exit criteria for each test stage.
6. Test plans clearly identify and document the test coverage, test scenarios and test conditions required to meet the objectives of that test stage, with appropriately skilled and knowledgeable resources used to develop the test plans (e.g., end users involved in creating user acceptance tests).
7. Test plans include, but are not limited to, a description of the test objective, the conditions required to execute the test, the test data required, the expected result and test result history. Test data accurately reflect the data to be processed in production without contravening local statutes and regulations concerning data privacy.
8. Errors and queries identified during testing are documented, prioritised, assessed and auditable. The assessment separates errors from enhancements, with the latter being addressed through the project scope change control process, where appropriate.
9. Summary results of testing are documented and auditable, with management information highlighting current progress, error detection and trends reported to appropriate project management. The impact of testing progress on the test plan is regularly assessed, with the test plan and the master project plan updated accordingly.
10. Test plans provide appropriate coverage of the organisation's business cycles, including, but not limited to, daily, weekly, monthly, quarterly, and financial and calendar year-end processes.

PO10.12 Training Plan

Why Do It?

Developing and executing a training plan in line with the control practices will:

- Increase the likelihood that end users will feel committed to, and confident in, using the project's deliverables
- Reduce the risk of manual errors arising after the project goes live
- Enable a wider community the opportunity to review and comment on the project's deliverables prior to go-live
- Enable IT staff to develop new skills required to develop, support and operate the project's deliverables post-go-live

Control Practices

1. A training plan is created for projects that will change working practices, either for end users or IT operations.
2. The training plan considers requirements for all training, including, but not limited to, end-user training, IT operations and support training, and IT application development training.
3. The training plan is an integral part of the overall project master plan, with clearly identified and understood resources, key milestones, dependencies and critical path tasks impacting the delivery of the training plans.
4. Alternative training strategies that satisfy the training requirements are considered, and the most cost-effective approach that aligns with the organisation's training framework is selected. Alternative strategies include train the trainer, end-user accreditation and intranet-based training.

PO10.13 Post-implementation Review Plan

Why Do It?

Developing and executing a post-implementation review plan in line with the control practices will:

- Assist in confirming that the project realises expected and agreed business benefits
- Identify project management and/or system development process improvements for future projects
- Provide a mechanism for assessing the project management framework and identifying improvement points
- Identify business process improvement suggestions for consideration in future project planning exercises

Figure 31—Control Practices for *Manage Projects (cont.)*

Control Practices

1. A post-implementation review is planned and executed to determine if the project has delivered expected benefits.
2. The post-implementation review considers opportunities for additional business value from further business process or system changes, and causal analysis of the strengths and weaknesses of the project management and system development approaches for the benefit of future developments. Improvements to the project management approach are reflected as changes to the project management framework.
3. The post-implementation review considers, but is not limited to, benefits realised, objectives met (including consideration of critical success factors and key performance indicators), development costs and timelines, outstanding documentation, open risk and issue log entries, outstanding defects and deferred scope items, and development and system quality.
4. The review considers the original project definition, approval documentation and subsequent changes agreed by the project board through the scope change control process.
5. The post-implementation review captures the views of key stakeholders, including leaders of affected business areas, the project team, project sponsor and other key project interfaces.
6. The review is conducted in a timely manner (e.g., within three months) following completion of the project and is led by a credible and impartial facilitator. If it is not possible to assess all critical success factors in such a time frame, then a smaller-scale follow-up review is scheduled for an appropriate time.

Figure 32—Audit Guidelines for *Manage Projects*

PO10 Manage Projects

Control Objectives	
1	Project management framework
2	User department participation in project initiation
3	Project team membership and responsibilities
4	Project definition
5	Project approval
6	Project phase approval
7	Project master plan
8	System quality assurance plan
9	Planning of assurance methods
10	Formal project risk management
11	Test plan
12	Training plan
13	Post-implementation review plan

BOTH HIGH-LEVEL AND DETAILED CONTROL OBJECTIVES ARE AUDITED BY:

Obtaining an understanding by:

- **Interviewing:**

  Quality manager
  Project quality manager/coordinator
  Project owners/sponsors
  Project team leader
  Quality assurance coordinator
  Security officer
  IT planning/steering committee members
  IT management

- **Obtaining:**

  Policies and procedures related to the project management framework
  Policies and procedures related to the project management methodology
  Policies and procedures related to quality assurance plans
  Policies and procedures related to quality assurance methods
  Software project master plan (SPMP)
  Software quality assurance plan (SQAP)
  Project status reports
  Status reports and minutes of planning/steering committee meetings
  Project quality reports

Figure 32—Audit Guidelines for *Manage Projects (cont.)*

Evaluating the controls by:

► **Considering whether:**

The project management framework:

- Defines scope and boundaries for managing projects
- Provides for project requests to be reviewed for their consistency with the approved operational plan and projects prioritised according to this plan
- Defines the project management methodology to be adopted and applied to each project undertaken, including:
  - Project planning
  - Staffing
  - Allocation of responsibilities and authorities
  - Task breakdown
  - Budgeting of time and resources
  - Milestones
  - Checkpoints
  - Approvals
- Is complete and current
- Provides for participation by the affected user department (owner/sponsor) management in the definition and authorisation of a development, implementation or modification project
- Specifies the basis on which staff members are assigned to projects
- Defines responsibilities and authorities of project team members
- Provides for the creation of a clear written statement defining the nature and scope of the project before work on the project begins
- Provides for an initial project definition document that includes a clear statement of the nature and scope of the project
- Includes the following reasons for undertaking the project:
  - A statement of the problem to be remedied or process to be improved
  - A statement of the need for the project expressed in terms of enhancing the organisation's ability to achieve its goals
  - An analysis of the deficiencies in relevant existing systems
  - The opportunities that would be provided for increasing economy or efficiency of operation
  - The internal control and security need that would be satisfied by the projects
- Addresses the manner in which proposed project feasibility studies are to be prepared, reviewed and approved by senior management, including the:
  - Environment of the project—Hardware, software, telecommunications
  - Scope of the project—What it will include and exclude in the first and following implementations
  - Constraints of the project—What must be retained during this project, even if short-term improvement opportunities seem apparent
  - Benefits and costs to be realised by the project sponsor or owner/sponsor
- Delineates the manner in which each phase of the development process (i.e., preparation of feasibility study, requirements definition, system design, etc.) is to be approved prior to proceeding to the next phase of the project (i.e., programming, system testing, transaction testing, parallel testing, etc.)
- Requires the development of software project management plan for each project and specifies the manner in which control, project time frames (milestones) and budgets will be maintained throughout the life of the project

Figure 32—Audit Guidelines for *Manage Projects (cont.)*

- Complies with either the organisation standard for SPMPs or, if none exists, an appropriate standard is used
- Requires the development of an software quality assurance plan for each project and ensures that this is integrated with the SPMP and formally reviewed and agreed by all involved parties
- Delineates the manner in which the formal project risk management programme eliminates or minimises the risks associated with the project
- Provides for the development of a test plan for every development, implementation and modification project
- Provides for the development of an adequate plan for training the owner/sponsor staff and IT staff for every development, implementation and modification project

Budgeted vs. actual project milestones and costs are monitored and reported to senior management throughout every major project phase (i.e., software purchase, hardware purchase, contract programming, network upgrades, etc.)

Project milestones and costs in excess of budgeted time frames and amounts are required to be approved by appropriate organisation management

SQAP complies with either the organisation standard for SQAPs or, if none exists, the criteria selected above

SQAP assurance tasks support the accreditation of new or modified systems and assure that internal controls and security features meet requirements

All project owners/sponsors had input into the SPMP and SQAP and all agreed final deliverables

The post-implementation process is an integral part of the project management framework to ensure that new or modified information systems have delivered the planned benefits

Assessing the compliance by:

► **Testing that:**

Project management methodology and all requirements were consistently followed

The project management methodology was communicated to all appropriate personnel involved in the project

The written definition of the nature and scope of the project conforms to a standard template

The owner/sponsor was involved in the project definition and authorisation, and the nature and extent of the involvement was in conformance with expected owner/sponsor involvement as provided for by the project management framework

Assignment of staff members to the project and definition of responsibilities and authorities of the project team members are being adhered to

A clear, written definition of the nature and scope of the project exists and is defined before work on the project begins

A relevant feasibility study has been prepared and approved

Appropriate owner/sponsor and IT management approvals are obtained for each phase of the development project

Each phase of the project is being completed and appropriate sign-off is occurring as required by the SPMP

SPMP and SQAP are developed and approved in accordance with the project management framework

SPMP and SQAP are detailed and specific enough

Mandatory activities/reports identified have in fact been executed/produced (i.e., executive steering committee meetings, project meetings or the like are held at set intervals, minutes of the meetings are taken and distributed to relevant parties, and reports are prepared and distributed to relevant parties)

The test plan has been developed and approved in accordance with the project management framework and is detailed and specific enough

Mandatory activities/reports identified in the test plan have in fact been executed/produced

Figure 32—Audit Guidelines for *Manage Projects (cont.)*

Accreditation criteria used for the project exist and:

- Are derived from goals and performance indicators
- Are derived from agreed-upon quantitative requirements
- Assure internal control and security requirements are met
- Are related to the essential "what" vs. the arbitrary "how"
- Define a formal pass/fail process
- Are capable of objective demonstration within a limited time period
- Do not simply restate requirements of design documents

The project risk management programme was used to identify and eliminate, or at least minimise, risks associated with the project

The test plan was adhered to, written testing reviews were created by the owner/sponsor, programming and quality assurance functions, and the sign-off process was complied with as intended

The written plan for training the staff of the affected owner/sponsor and IT functions was prepared, it allowed sufficient time for completing the required training activities, and the plan was used for the project

The post-implementation review plan was adhered to and carried out for the project

Substantiating the risk of control objectives not being met by:

► **Performing:**

Benchmarking of the project management framework against similar organisations or appropriate international standards/recognised industry best practices

A detailed review of:

- The project master plan to determine the extent of owner/sponsor participation and the adequacy of the general process of defining, authorising and executing the project, including:
  - Definition of system functions
  - Feasibility, given constraints of the project
  - Determination of system costs and benefits
  - Appropriateness of system controls
  - Impact and integration in other owner/sponsor systems
  - Owner/sponsor commitment of resources (people and money)
  - Definition of responsibilities and authorities of project participants
  - Acceptance criteria are desirable and achievable
  - Use of milestones and checkpoints in authorising the various project phases
  - Use of Gantt charts, problem logs, meeting summaries, etc., in managing the project
- Quality reports to determine if systemic problems exist in the organisation's system quality assurance planning process
- The formal project risk management programme to determine if risks have been identified and eliminated, or at least minimised
- The execution of the test plan to determine that it thoroughly tested the entire system development, implementation or modification project
- The execution of the training plan to determine that it adequately prepared the owners/sponsors and IT staff in the use of the system
- The post-implementation review to determine if planned vs. delivered benefits of the project were ascertained

Figure 32—Audit Guidelines for *Manage Projects (cont.)*

► **Identifying:**

Projects that:

- Are poorly managed
- Exceed milestone dates
- Exceed costs
- Are runaway projects
- Have not been authorised
- Are not technically feasible
- Are not cost-justified
- Do not achieve planned benefits
- Do not contain checkpoints
- Are not approved at key checkpoints
- Are not accredited for implementation
- Do not meet internal control and security requirements
- Do not eliminate or mitigate risk
- Have not been thoroughly tested
- Needed training, which has not occurred or is inadequate for the system being implemented
- Have not undergone a post-implementation review

Figure 33—Management Guidelines for *Manage Projects*

PO10 Plan and Organise
Manage Projects

Control over the IT process ***manage projects*** with the business goal of setting priorities and delivering on time and within budget

ensures delivery of information to the business that addresses the required information criteria and is measured by key goal indicators

is enabled by the organisation identifying and prioritising projects in line with the operational plan and the adoption and application of sound project management techniques for each project undertaken

considers critical success factors that leverage specific IT resources and is measured by key performance indicators

Information Criteria	
P	Effectiveness
P	Efficiency
	Confidentiality
	Integrity
	Availability
	Compliance
	Reliability

(**P**) primary (**S**) secondary

IT Resources	
✓	People
✓	Applications
✓	Technology
✓	Facilities
	Data

(✓) applicable to

Critical Success Factors

- Experienced and skilled project managers are available.
- An accepted and standard programme management process is in place.
- There is senior management sponsorship of projects, and stakeholders and IT staff share in the definition, implementation and management of projects.
- There is an understanding of the abilities and limitations of the organisation and the IT function in managing large, complex projects.
- An organisationwide project risk assessment methodology is defined and enforced.
- All projects have a plan with clear, traceable work breakdown structures, reasonably accurate estimates, skill requirements, issues to track, a quality plan and a transparent change process.
- The transition from the implementation team to the operational team is a well-managed process.
- A system development life cycle methodology has been defined and is used by the organisation.

Key Goal Indicators

- Increased number of projects completed on time and on budget
- Availability of accurate project schedule and budget information
- Decrease in systemic and common project problems
- Improved timeliness of project risk identification
- Increased organisation satisfaction with project delivered services
- Improved timeliness of project management decisions

Key Performance Indicators

- An increase in the number of projects delivered in accordance with a defined methodology
- Percent of stakeholder participation in projects (involvement index)
- Number of project management training days per project team member
- Number of project milestone and budget reviews
- Percent of projects with post-project reviews
- Average number of years of experience of project managers

Figure 33—Management Guidelines for *Manage Projects (cont.)*

PO10 Maturity Model

Control over the IT process ***manage projects*** with the business goal of setting priorities and delivering on time and within budget

0 **Nonexistent**—Project management techniques are not used and the organisation does not consider business impacts associated with project mismanagement and development project failures.

1 **Initial/*Ad Hoc***—The organisation is generally aware of the need for projects to be structured and is aware of the risks of poorly managed projects. The use of project management techniques and approaches within IT is a decision left to individual IT managers. Projects are generally poorly defined and do not incorporate business and technical objectives of the organisation or the business stakeholders. There is a general lack of management commitment and project ownership and critical decisions are made without user management or customer input. There is little or no customer and user involvement in defining IT projects. There is no clear organisation within IT projects, and roles and responsibilities are not defined. Project schedules and milestones are poorly defined. Project staff time and expenses are not tracked and compared to budgets.

2 **Repeatable but Intuitive**—Senior management has gained and communicated an awareness of the need for IT project management. The organisation is in the process of learning and repeating certain techniques and methods from project to project. IT projects have informally defined business and technical objectives. There is limited stakeholder involvement in IT project management. Some guidelines have been developed for most aspects of project management, but their application is left to the discretion of the individual project manager.

3 **Defined Process**—The IT project management process and methodology have been formally established and communicated. IT projects are defined with appropriate business and technical objectives. Stakeholders are involved in the management of IT projects. The IT project organisation and some roles and responsibilities are defined. IT projects have defined and updated milestones, schedules, budget and performance measurements. IT projects have formal post-system-implementation procedures. Informal project management training is provided. Quality assurance procedures and post-system-implementation activities have been defined, but are not broadly applied by IT managers. Policies for using a balance of internal and external resources are being defined.

4 **Managed and Measurable**—Management requires formal and standardised project metrics and lessons learned to be reviewed following project completion. Project management is measured and evaluated throughout the organisation and not just within IT. Enhancements to the project management process are formalised and communicated, and project team members are trained on all enhancements. Risk management is performed as part of the project management process. Stakeholders actively participate in the projects or lead them. Project milestones, as well as the criteria for evaluating success at each milestone, have been established. Value and risk are measured and managed prior to, during and after the completion of projects. Management has established a programme management function within IT. Projects are defined, staffed and managed to increasingly address organisation goals, rather than only IT-specific goals.

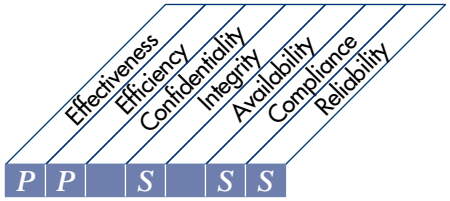
5 **Optimised**—A proven, full life cycle project methodology is implemented, enforced and integrated into the culture of the entire organisation. An ongoing programme to identify and institutionalise best practices has been implemented. There is strong and active project support from senior management sponsors as well as stakeholders. IT management has implemented a project organisation structure with documented roles, responsibilities and staff performance criteria. A long-term IT resources strategy is defined to support development and operational outsourcing decisions. An integrated programme management office is responsible for projects from inception to post-implementation. The programme management office is under the management of the business units and requisitions and directs IT resources to complete projects. Organisationwide planning of projects ensures that user and IT resources are best utilised to support strategic initiatives.

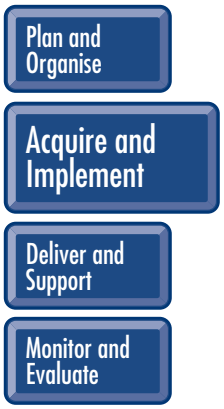
Figure 34—Control Objectives for *Acquire and Maintain Application Software*

HIGH-LEVEL CONTROL OBJECTIVE

AI2 Acquire and Implement

Acquire and Maintain Application Software





Control over the IT process of

acquiring and maintaining application software

that satisfies the business requirement

to provide automated functions that effectively support the business process

is enabled by

the definition of specific statements of functional and operational requirements and a phased implementation with clear deliverables

and takes into consideration

- Functional testing and acceptance
- Application controls and security requirements
- Documentation requirements
- Application software life cycle
- Enterprise information architecture
- System development life cycle methodology
- User-machine interface
- Package customisation

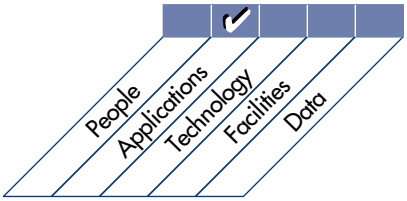


Figure 34—Control Objectives for *Acquire and Maintain Application Software (cont.)*

DETAILED CONTROL OBJECTIVES

2 ACQUIRE AND MAINTAIN APPLICATION SOFTWARE

2.1 **Design Methods**
CONTROL OBJECTIVE
The organisation's system development life cycle methodology should ensure that appropriate procedures and techniques, involving close liaison with system users, are applied to create the design specifications for each new information system development project and verify the design specifications against the user requirements.

2.2 **Major Changes to Existing Systems**
CONTROL OBJECTIVE
Management should ensure that, in the event of major changes to existing systems, a similar development process is observed as in the case of the development of new systems.

2.3 **Design Approval**
CONTROL OBJECTIVE
The organisation's system development life cycle methodology should require that the design specifications for all information system development and modification projects be reviewed and approved by management, the affected user departments and the organisation's senior management, when appropriate.

2.4 **File Requirements Definition and Documentation**
CONTROL OBJECTIVE
The organisation's system development life cycle methodology should ensure that an appropriate procedure is applied for defining and documenting the file format for each information system development or modification project. Such a procedure should ensure that the data dictionary rules are respected.

2.5 **Program Specifications**
CONTROL OBJECTIVE
The organisation's system development life cycle methodology should require that detailed written program specifications are prepared for each information system development or modification project. The methodology should further ensure that program specifications agree with system design specifications.

2.6 **Source Data Collection Design**
CONTROL OBJECTIVE
The organisation's system development life cycle methodology should require that adequate mechanisms for the collection and entry of data are specified for each information system development or modification project.

2.7 **Input Requirements Definition and Documentation**
CONTROL OBJECTIVE
The organisation's system development life cycle methodology should require that adequate mechanisms exist for defining and documenting the input requirements for each information system development or modification project.

2.8 **Definition of Interfaces**
CONTROL OBJECTIVE
The organisation's system development life cycle methodology should ensure that all external and internal interfaces are properly specified, designed and documented.

2.9 **User-machine Interface**
CONTROL OBJECTIVE
The organisation's system development life cycle methodology should provide for the development of an interface between the user and machine that is easy to use and self-documenting (by means of online help functions).

continued on next page

Figure 34—Control Objectives for *Acquire and Maintain Application Software (cont.)*

2.10 **Processing Requirements Definition and Documentation**
CONTROL OBJECTIVE
The organisation's system development life cycle methodology should require that adequate mechanisms exist for defining and documenting the processing requirements for each information system development or modification project.

2.11 **Output Requirements Definition and Documentation**
CONTROL OBJECTIVE
The organisation's system development life cycle methodology should require that adequate mechanisms exist for defining and documenting the output requirements for each information system development or modification project.

2.12 **Controllability**
CONTROL OBJECTIVE
The organisation's system development life cycle methodology should require that adequate mechanisms for assuring the internal control and security requirements be specified for each information system development or modification project. The methodology should further ensure that information systems are designed to include application controls that guarantee the accuracy, completeness, timeliness and authorisation of inputs, processing and outputs. Sensitivity assessment should be performed during the initiation of system development or modification. The basic security and internal control aspects of a system to be developed or modified should be assessed along with the conceptual design of the system to integrate security concepts in the design as early as possible.

2.13 **Availability as a Key Design Factor**
CONTROL OBJECTIVE
The organisation's system development life cycle methodology should ensure that availability is considered in the design process for new or modified information systems at the earliest possible stage. Availability should be analysed and, if necessary, increased through maintainability and reliability improvements.

2.14 **IT Integrity Provisions in Application Program Software**
CONTROL OBJECTIVE
The organisation should establish procedures to assure, where applicable, that application programs contain provisions that routinely verify the tasks performed by the software to help assure data integrity, and provide the restoration of integrity through rollback or other means.

2.15 **Application Software Testing**
CONTROL OBJECTIVE
Unit testing, application testing, integration testing, system testing, and load and stress testing should be performed according to the project test plan and established testing standards, before the application software is accepted by the user. Adequate measures should be conducted to prevent disclosure of sensitive information used during testing.

2.16 **User Reference and Support Materials**
CONTROL OBJECTIVE
The organisation's system development life cycle methodology should ensure that adequate user reference and support manuals are prepared (preferably in electronic format) as part of every information system development or modification project.

2.17 **Reassessment of System Design**
CONTROL OBJECTIVE
The organisation's system development life cycle methodology should ensure that the system design is reassessed whenever significant technical and/or logical discrepancies occur during system development or maintenance.

Figure 35—Control Practices for *Acquire and Maintain Application Software*

AI2.1 Design Methods

Why Do It?
The provision of proper design methods in line with the control practices will:
- Ensure that the design matches the requirements
- Generate clear design specifications thereby reducing cost and time to delivery
- Ensure consistency between the physical design and logical design
- Avoid single points of dependency (e.g., dependency on the designers)

Control Practices
1. The organisation has design standards and a method to verify compliance with the standard. The design standards address the design of output, files, database access, input, control procedures and program specifications.
2. The design is consistent with the business plans and strategies and the information technology plans; other supporting documents are unambiguously cross-referenced by title and date.
3. There is a process to ensure that detailed design specifications reflect user (functional and operational) requirements and provide for file and transaction controls commensurate with risk.
4. The design results in specifications for hardware, software, processing logic, input/output requirements, media, and manual procedures and controls.
5. The logical and physical design specifications are complete and clear so that the reader, without prior background of the project, is able to understand the specifications.
6. Users are involved in the design process to draw on their expertise and knowledge of the current system or processes.

AI2.2 Major Changes to the Existing Systems

Why Do It?
Controlling major changes to the existing systems along the lines of the control practices will:
- Ensure proper risk management to maximise system availability, integrity of processing, and confidentiality and integrity of data
- Ensure consistency in the approach for major development undertakings and thereby increase predictability of quality and cost

Control Practices
1. The system development methodology requires all changes to be classified according to specified, objective criteria, reflecting the risk involved.
2. All major changes are treated as new systems, as far as the required procedures for acquiring and maintaining application software are concerned.

AI2.3 Design Approval

Why Do It?
Design approvals performed in line with the control practices will:
- Ensure the designed solution can be implemented, operated and maintained and matches the approved requirements
- Establish a formal checkpoint before initiating the development
- Fix the scope of the development work, allowing adequate project planning

Control Practices
1. The development methodology requires a formal checkpoint for the review and approval of the design. No project proceeds into development without appropriate sign-off.
2. The design specifications are approved and signed off by the stakeholders (e.g., end users, operations staff, security experts) to ensure that their expectations have been incorporated and the design, as a whole, constitutes a solution that the organisation can deliver, operate and maintain.
3. The final design specifications, after review and quality assurance, are submitted to the project sponsor for approval and sign-off.
4. Where appropriate, senior management and information technology management approve the initial definition and give approval to proceed to the next stage. The development methodology is formalised, which requires this final sign-off.

AI2.4 File Requirements Definition and Documentation

Why Do It?
An effective file requirement definition and documentation procedure in line with the control practices will:
- Ensure data are consistently stored in unique places, avoiding potential loss of integrity due to partial updates
- Ensure consistency with the organisationwide data dictionary
- Facilitate efficient program maintenance

Control Practices
1. Common data dictionary standards are created for the organisation. The standards document the methodology for storage, location and retrieval of records and take into consideration the predominant use of the data within the organisation.

Figure 35—Control Practices for *Acquire and Maintain Application Software (cont.)*

2. A procedure ensures that data storage requirements for individual projects are in line with the organisation's data dictionary standards.
3. Clear instructions are available for naming database objects, including tables, views, columns and indices, and they follow the naming conventions imposed by the programming languages used.
4. The file requirements definition documents the methodology for storage, location and retrieval of records.

AI2.5 Program Specifications

Why Do It?
Program specifications in line with the control practices will:
- Facilitate program maintenance
- Maximise development efficiency by promoting the use of shared routines

Control Practices
1. The organisation ensures that well-defined program specifications are available for every project and they follow the design.
2. Procedures ensure that a repository of shared routines or reusable components exists and the solution design refers to it. The reuse of existing code is required where appropriate.

AI2.6 Source Data Collection Design

Why Do It?
An efficient source data collection methodology and design in line with the control practices will:
- Ensure that all essential data are captured once and only once throughout the organisation
- Avoid costly system redesign because important and valuable data were omitted
- Ensure timely processing
- Prevent loss, modification or misuse of data in application systems

Control Practices
1. Source data collection design clearly specifies the data that must be collected and validated for processing transactions as well as the methods for validation.
2. Source data collection design optimises throughput, ensuring that no data are lost because of inadequate performance of the data collection system.
3. The SDLC methodology provides for the proper formalisation of data validation rules, by comparison to standing data, reasonability checks or mathematical verification.

AI2.7 Input Requirements Definition and Documentation

Why Do It?
An effective input requirements definition and documentation methodology in line with the control practices will:
- Remove performance inefficiencies due to nonalignment of data capture methods and the data source
- Prevent invalid transactions from being entered and prevent invalid data within valid transactions
- Ensure that the errors identified during data capture are effectively handled

Control Practices
1. The input requirements definition provides for a method of data capture adapted to the data source and the subsequent use of the captured data.
2. The input requirements definition specifies all data sources, including previously stored as well as computed data.
3. The input requirements definition specifies the input validation method so that only valid data and transactions are processed. When errors are detected, automatic correction facilities are provided, to the extent possible.
4. The input requirements definition reflects the approach for input error handling.

AI2.8 Definition of Interfaces

Why Do It?
Definition of interfaces in line with the control practices will:
- Avoid costly amendments to the design
- Ensure that system boundaries are effectively mapped, and the impact of the interfaces are properly assessed and considered

Control Practices
1. Before finalising the preliminary system level requirements, an inventory of all interfaces is completed.
2. The definition of interfaces includes source, format, structure, content and method of support.

AI2.9 User-machine Interface

Why Do It?
A reliable user-machine interface in line with the control practices will:
- Reduce help desk costs
- Provide effective guidance to users on ways to fix issues

Figure 35—Control Practices for *Acquire and Maintain Application Software (cont.)*

Control Practices
1. Context-sensitive help is available for all screens, input fields, dialogue boxes and functions.
2. The design of the help function (content, structure and focus) helps the user fix a problem or complete a task as quickly as possible. It does not show the user how to perform the task.

AI2.10 Processing Requirements Definition and Documentation

Why Do It?
An effective processing requirements definition procedure and documentation in line with the control practices will:
- Maximise coding efficiency
- Ensure long-term maintainability of the software
- Minimise the possibility of data corruption

Control Practices
1. The processing logic is documented in a way that is understandable for nontechnical people (pseudocode, flowcharts, etc.), whilst containing sufficient detail to allow accurate coding by the programmers.
2. Software contains internal documentation. Descriptive comments are embedded within the body of the source code and are used to describe the processing functions. The comments include cross-references to the design and requirements.
3. The processing requirements include validation checks capable of detecting data that have been corrupted by processing errors or through deliberate acts.
4. The processing requirements lay out the sequence of programs as well as steps to be taken in case of a processing failure.

AI2.11 Output Requirements Definition and Documentation

Why Do It?
Defining and documenting output requirements in line with the control practices will:
- Focus on the important features of the information generated
- Ensure that the reports generated meet the business requirements
- Ensure that the reports are relevant so there will be no loss of time and resources due to the delay in locating information
- Ensure that output is correct and appropriate to the circumstances

Control Practices
1. The output requirements definition is based on the user requirements and should take into account the different types of recipients, usage, details required, frequency, method of generation and other design details.
2. The output requirements definition documents the general type of output format, which will enable clear, concise and readable presentation where applicable.
3. Requirements for output validation are determined so accuracy and completeness can be verified.
4. The classification of the output is clearly indicated, and appropriate measures to guarantee availability, integrity and confidentiality are proposed.

AI2.12 Controllability

Why Do It?
Controllability in line with the control practices will:
- Ensure that, with formal specification of the controls, most of the security issues are appropriately considered and implemented before system implementation
- Prevent the need to add (possibly costly) controls at a later stage of implementation

Control Practices
1. The SDLC methodology specifically solicits control and security requirement specifications from the users at the time business functional requirements are sought. This covers adequate internal controls and security as well as application controls over accuracy, completeness, timeliness and authorisation.
2. The application control specifications ensure compliance with the security policy of the organisation.

AI2.13 Availability as a Key Design Factor

Why Do It?
Considering availability as a key design factor in an SDLC methodology in line with the control practices will:
- Provide the required robustness and the maximum uptime for the application
- Ensure that the application can perform on various platforms
- Avoid the costs of redesigning to add availability to an existing system

Control Practices
1. The SDLC methodology includes a step for gathering availability requirements. Once this is known, the impact on redundancy, failures and backup processing is formulated.
2. The SDLC methodology specifies requirements for maintainability, stressing the importance of appropriate documentation (external and internal) and modularity.
3. The SDLC methodology maximises the ability of all the systems to operate on multiple platforms.

Figure 35—Control Practices for *Acquire and Maintain Application Software (cont.)*

4. The SDLC methodology requires adequate documentation of file and database formats, program source code and logic to improve long-term maintainability and, hence, overall availability by reducing downtime.

AI2.14 Information Technology Integrity Provisions in Application Program Software

Why Do It?
Providing information technology integrity provisions in application software in line with the control practices will:
- Ensure data integrity
- Ensure program integrity at source code and object/executable level
- Minimise the need for manual reconciliation (which may be impossible due to volumes of data)

Control Practices
1. Any database management system is configured to use all available integrity mechanisms (e.g., protecting referential integrity). Upon detection of data corruption, rollback is possible.
2. Integrity of data in process is guaranteed. This is done by verifying digital signatures.
3. Program integrity is ensured on the source code level by using adequately configured source code repositories, and on the production system level by implementing a system that will verify system content with a baseline established at system installation (and updated for authorised system changes).

AI2.15 Application Software Testing

Why Do It?
Reliable application software testing procedures in line with the control practices will:
- Provide for effective testing mechanisms and eliminate retesting due to poor documentation
- Prevent deviation from standard testing methodology of the organisation and identify bugs at an early stage rather than at a (potentially more costly) later stage
- Ensure that the data used for testing purposes are relevant to the business situations and the testing is not compromised by development team members also participating on the testing team
- Prevent misuse of test data for committing frauds resulting in legal liabilities and damage to reputation
- Ensure that all types of users perform testing and formally accept the software

Control Practices
1. The organisation's test standards are well documented with requirements to perform for various types of tests (e.g., unit testing, integration testing, load and stress testing, acceptance testing, regression testing), responsibility for documentation, review, and approval of test and test results. Testing is extended to cover online help functions and user manuals as well as installation and operational guidelines.
2. Test results are retained for subsequent review.
3. The choice between live data or generated test data is based on the circumstances. Test data are representative of live data in quality (valid/invalid) and volume.
4. An independent team of testers, other than those involved in development, perform the tests. Tests are performed on executables received from the central release management authority.
5. Prior to testing, a test plan walk-through is carried out to ensure the adequacy of the test plan. This reviews compliance with the organisation's standards, test scenarios, testing participants' responsibilities, acceptance criteria and testing logistics. Test cases (and the expected results) are documented for every condition and option.
6. Specific tests are designed to detect unauthorised changes.
7. Prior to system testing, a code review is carried out to ensure adherence of program to design, coding and naming conventions.
8. Test results are kept and any problems are prioritised and followed up for correction.
9. Integrity and confidentiality of test data/test results are guaranteed.
10. End users or system owners verify that the appropriate testing has been performed with expected results. This includes approval that all requirements have been successfully tested.
11. Senior management sign-off is required when programs are promoted to production with known errors.

AI2.16 User Reference and Support Materials

Why Do It?
Availability of approved user reference and support materials in line with the control practices will:
- Ensure that all types of users are provided with adequate, up-to-date documentation

Figure 35—Control Practices for *Acquire and Maintain Application Software (cont.)*

Control Practices
1. A procedure ensures the availability of approved user reference materials and support materials before acceptance.
2. The various types of user and reference materials are designed for all levels of expertise. The user reference manuals are simple, inform users about the general use of the application program and provide information on commands and their use. Electronic documentation is preferred.

AI2.17 Reassessment of System Design

Why Do It?
Providing for reassessment of system design after the initial implementation in line with control practices will ensure that:
- Systems and their design are kept up to date
- Decisions to reassess system design are justified

Control Practices
1. The SDLC methodology provides guidelines for identifying/defining major discrepancies that would trigger reassessment of the system design.
2. When the need for reassessment is identified, the design is effectively completed.

Figure 36—Audit Guidelines for *Acquire and Maintain Application Software*

AI2 ACQUIRE AND MAINTAIN APPLICATION SOFTWARE

CONTROL OBJECTIVES	
1	Design methods
2	Major changes to existing systems
3	Design approval
4	File requirements definition and documentation
5	Program specifications
6	Source data collection design
7	Input requirements definition and documentation
8	Definition of interfaces
9	User-machine interface
10	Processing requirements definition and documentation
11	Output requirements definition and documentation
12	Controllability
13	Availability as a key design factor
14	IT integrity provisions in application program software
15	Application software testing
16	User reference and support materials
17	Reassessment of system design

BOTH HIGH-LEVEL AND DETAILED CONTROL OBJECTIVES ARE AUDITED BY:

Obtaining an understanding by:

► **Interviewing:**

Chief information officer
Security officer
IT senior management
Project owners/sponsors

► **Obtaining:**

Policies and procedures relating to the system development life cycle methodology
IT objectives and long- and short-range plans
Selected project documentation, including design approvals, file requirements definition, program specifications, source data collection design, input requirements definition, user-machine interface, processing requirements definition, output requirements definition, internal control/security requirements, availability requirements, IT integrity provisions, application software test plan and results, user reference and support materials, and reassessment of system design

Figure 36—Audit Guidelines for *Acquire and Maintain Application Software (cont.)*

Evaluating the controls by:

► **Considering whether:**

Policies and procedures ensure that:

- The organisation's system development life cycle methodology applies to the development of new systems and major changes to existing systems and user participation
- Close liaison with the user exists in creating the design specifications and verifying the design specifications against user requirements
- In the event of major changes to existing systems, a similar system development life cycle process is observed, as in the case of the development of new systems
- Design specifications are signed off by management, the affected user departments and the organisation's senior management, when appropriate, for all new system development and modification projects
- An appropriate process is applied for defining and documenting the file format for each new system development or modification project, including a requirement that the data dictionary rules are respected
- Detailed written program specifications are prepared for each information development or modification project and these program specifications agree with the system design specifications
- Adequate mechanisms for the collection and entry of data are specified for each new system development or modification project
- Adequate mechanisms for defining and documenting the input requirements for each new system development or modification project exist
- An interface between the user and the machine exists that is easy to use and self-documenting (by means of online help functions)
- Adequate mechanisms for defining and documenting internal and external interfaces for each new system development or modification project exist
- Adequate mechanisms for defining and documenting the processing requirements for each new system development or modification project exist
- Adequate mechanisms for defining and documenting the output requirements for each new system development or modification project exist
- Adequate mechanisms for ensuring internal control and security requirements are specified for each new system development or modification project
- The internal control and security requirements include application controls that guarantee the accuracy, completeness, timeliness and authorisation of inputs and outputs
- Availability is considered in the design process of new or modified systems at the earliest possible stage, and this consideration analyses and, if necessary, increases through maintainability and reliability improvements
- Applications programs contain provisions that routinely verify the tasks performed by the software and provide restoration of integrity through rollback or other means
- Application software is tested according to the project test plan and established testing standards before being approved by the user
- Adequate user reference and support manuals are prepared (preferably in electronic format) as part of every system development or modification process
- The system design is reassessed whenever significant technological and/or logical discrepancies occur during system development or maintenance

The system development life cycle methodology ensures that user reference and support materials are updated in an accurate and timely manner

A sensitivity assessment is required by the system development life cycle methodology to be performed during the initiation of new system development or modification

Figure 36—Audit Guidelines for *Acquire and Maintain Application Software (cont.)*

System development life cycle methodology requires that basic security and internal control aspects of a new system to be developed or modified be assessed along with the conceptual design of the system to integrate security concepts in the design as early as possible

Logical security and application security issues are required by the system development life cycle methodology to be addressed and included in the design of new systems or modifications of existing ones

The assessment of the security and internal control aspects is based on a sound framework

Artificial intelligence systems are placed in an interaction or control framework with human operators to ensure that vital decisions are approved

Disclosure of sensitive information used during application testing is mitigated by either strong access limitations or depersonalisation of the used historical data

Assessing the compliance by:

► **Testing that:**

User participation in the system development life cycle process is high

The organisation's system development life cycle methodology ensures that a process is in place to appropriately address all system design issues (i.e., input, processing, output, internal controls, security, disaster recovery, response time, reporting, change control, etc.)

Key system users are involved in the system design process

The design, review and approval process ensures that all issues have been resolved prior to beginning work on the next phase of the project

Major changes to existing systems ensure that they are developed using a similar system development life cycle methodology to that used for the development of new systems

Design sign-off procedures are in place to ensure that programming of the system is not started until proper design sign-offs are obtained

System file requirements and documentation and data dictionary are all consistent with standards

User sign-off on final file specifications occurs

Program specifications agree with system design specifications

Data collection and data entry design specifications match

User-machine interface design specifications exist

User-machine specifications are easy to use and self-documenting (using online help facilities) functions are employed

Internal and external interfaces are documented

Processing requirements are in design specifications

Output requirements are in design specifications

Internal control and security requirements are in design specifications

Application control requirements design specifications guarantee the accuracy, completeness, timeliness and authorisation of inputs and outputs

Internal control and security requirements have been included in the conceptual design of the system (whether a new system or one being modified) as early as possible

The security officer is actively involved in the system design, development and implementation process of the new system or system modification project

The system design determines whether improved availability/reliability has been quantified in terms of time and more efficient procedures over prior methods if applicable

Application program provisions routinely verify the tasks performed by the software to help assure data integrity

Established testing standards exist

Figure 36—Audit Guidelines for *Acquire and Maintain Application Software (cont.)*

A project test plan and user approval process exist

User reference and support materials and an online help facility are available

The help desk function is effectively assisting users in addressing more complex processing issues

The process for escalating help desk issues includes the tracking, monitoring and reporting of such issues to appropriate IT management

A mechanism is in place to update user documentation

Communication of user documentation changes is occurring

A reassessment process is undertaken whenever significant technological and/or logical discrepancies occur

Substantiating the risk of the control objectives not being met by:

► **Performing:**

Benchmarking costs of acquiring and developing application software against similar organisations or appropriate international standards/recognised industry best practices

A detailed review of selected:

- System design documentation to evaluate the adequacy of the design specifications and adherence of the design to those specifications
- New system development or modification projects that determine whether design specification documents have been reviewed and approved by the management of the IT function and the affected user functions as well as the organisation's senior management, when appropriate
- Software documentation to ensure that file requirements (for at least those files listed below) are clearly understood by the project implementation team and are being structured per system and user requirements and the organisation's data dictionary rules:
  - Master
  - Transaction
  - Command
  - Program
  - Control
  - Table
  - Report
  - Print
  - Log
  - Transmission
- New system development and modification projects to ensure that files, program, source data collection instruments, inputs, user-machine interfaces, processing steps and outputs identified in flowcharts/flow diagrams correspond to the various system design specifications
- New system development and modification projects to determine that whenever significant technical and/or logical discrepancies are identified, an effective system design reassessment process occurs
- New system development and modification projects to determine the existence of any technical design discrepancies or functional changes needed
- New system development and modification projects and conceptual system designs to evaluate the adequacy of the internal control and security provisions that ensure the accuracy, completeness, timeliness and authorisation of inputs and outputs, and the integration of security concepts in the design at the earliest possible time

Figure 36—Audit Guidelines for *Acquire and Maintain Application Software (cont.)*

- New system development and modification projects to evaluate the design in light of improved availability and reliability for the end user and maintainability for IT maintenance personnel
- Projects to evaluate the adequacy of application program data integrity verification
- New system development and modification projects to ensure that user reference materials are current and consistent with the system documentation and fully meet user needs

A detailed review of the effectiveness of:

- The program specifications process to ensure that programs are written according to user design specifications
- The input specifications process to ensure that programs are written according to user design specifications
- The user-machine interface specifications process to ensure that programs are written according to user design specifications
- The processing specifications process to ensure that programs are written according to user design specifications
- The output specifications process to ensure that programs are written according to user design specifications

A detailed review of the organisation's testing standards and the implementation of associated test plans for selected new system development and modification projects

A detailed review of user satisfaction with the system, its reports, user documentation and reference materials, help facilities, etc.

► **Identifying:**

Deficiencies in the organisation's system development life cycle methodology used for new system development or modification projects

Design specifications that do not reflect user requirements

File requirements that are not consistent with the organisation's data dictionary rules

New system development or modification projects that contain inadequately defined file, program, source data selection, input, user-machine interface, processing, output and/or controllability requirements

New system development or modification projects where availability was not considered in the design process

Data integrity deficiencies in application program software in new system development or modification projects

Deficiencies in the organisation's testing standards that have resulted in the implementation of systems that do not process data correctly, report data incorrectly, etc.

Test plan deficiencies in new system development or modification projects

Deficiencies in user reference and support materials in new system development or modification projects

Significant technical and/or logical discrepancies that have occurred during system development or maintenance that did not result in reassessment of the system design and, therefore, went uncorrected or resulted in inefficient, ineffective and uneconomical patches to the system

Figure 37—Management Guidelines for *Acquire and Maintain Application Software (cont.)*

AI2 Acquire and Implement
Acquire and Maintain Application Software

Control over the IT process ***acquire and maintain application software*** with the business goal of providing automated functions that effectively support the business process

ensures delivery of information to the business that addresses the required information criteria and is measured by key goal indicators

is enabled by the definition of specific statements of functional and operational requirements, and a phased implementation with clear deliverables

considers critical success factors that leverage specific IT resources and is measured by key performance indicators

Information Criteria
P Effectiveness
P Efficiency
Confidentiality
S Integrity
Availability
S Compliance
S Reliability

(**P**) primary (**S**) secondary

IT Resources
People
✓ Applications
Technology
Facilities
Data

(✓) applicable to

Key Goal Indicators

- Number of applications delivered on time, meeting specifications and in line with the IT architecture
- Number of applications without integration problems during implementation
- Cost of maintenance per application below the set level
- Number of production problems per application, causing visible downtime or service degradation
- Number of solutions not consistent with the currently approved IT strategy
- Reduced ratio of maintenance efforts relative to new development

Critical Success Factors

- The acquisition and implementation methodology is strongly supported by senior management.
- Acquisition practices are clear, understood and accepted.
- There is a formal, accepted, understood and enforced acquisition and implementation methodology .
- An appropriate set of automated support tools is available, saving time on software selection by focusing on the best of breed.
- There is separation between development and testing activities.
- Key requirements are prioritised in view of possible scope reductions, if time, quality or cost cannot be compromised.
- The approach taken and effort committed are related to the business relevance of the application.
- The degree and form of documentation required are agreed and followed in the implementation.
- Compliance with corporate IT architecture is monitored, including a formal process for approving deviations.

Key Performance Indicators

- Ratio of actual maintenance cost per application vs. the application portfolio average
- Average time to deliver functionality, based on measures such as function point or modules
- Number of change requests related to bugs, critical errors and new functional specifications
- Number of production problems or disfunctionality per application and per maintenance change
- Number of deviations from standard procedures, such as undocumented applications, unapproved design and testing reduced to meet deadlines
- Number of returned modules or level of rework required after acceptance testing
- Time lag to analyse and fix problems
- Number or percent of application software effectively documented for maintenance

Figure 37—Management Guidelines for *Acquire and Maintain Application Software (cont.)*

AI2 Maturity Model

Control over the IT process ***acquire and maintain application software*** with the business goal of providing automated functions that effectively support the business process

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

1 **Initial/*Ad Hoc***—There is an awareness that a process for acquiring and maintaining applications is required. , However, approaches vary from project to project without any consistency and typically in isolation from other projects. The organisation is likely to have acquired a variety of individual solutions and now suffers legacy problems and inefficiencies with maintenance and support. The business users are unable to gain much advantage from IT investments.

2 **Repeatable but Intuitive**—There are similar processes for acquiring and maintaining applications, but they are based on the expertise within the IT function, not on a documented process. The success rate with applications depends greatly on the in-house skills and experience levels within IT. Maintenance is usually problematic and suffers when internal knowledge has been lost from the organisation.

3 **Defined Process**—There are documented acquisition and maintenance processes. An attempt is made to apply the documented processes consistently across different applications and projects, but they are not always found to be practical to implement or reflective of current technology solutions. They are generally inflexible and hard to apply in all cases, so steps are frequently bypassed. As a consequence, applications are often acquired in a piecemeal fashion. Maintenance follows a defined approach, but is often time-consuming and inefficient.

4 **Managed and Measurable**—There are a formal, clear and well-understood system acquisition and implementation methodology and policy that include a formal design and specification process, criteria for acquisition of application software, a process for testing and requirements for documentation, ensuring that all applications are acquired and maintained in a consistent manner. Formal approval mechanisms exist to ensure that all steps are followed and exceptions are authorised. The methods have evolved so that they are well suited to the organisation and are likely to be positively used by all staff, and applicable to most application requirements.

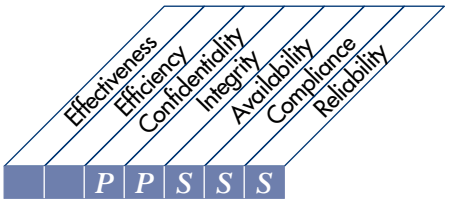
5 **Optimised**—Application software acquisition and maintenance practices are in line with the agreed processes. The approach is component-based, with predefined, standardised applications matched to business needs. It is usual for organisationwide approaches to be taken. The acquisition and maintenance process is well advanced, enables rapid deployment and allows for high responsiveness, as well as flexibility, in responding to changing business requirements. The application software acquisition and implementation process has been subject to continuous improvement and is supported by internal and external knowledge databases containing reference materials and best practices. The methodology creates computer-based documentation in a predefined structure that makes production and maintenance very efficient.

Figure 38—Control Objectives for *Ensure Systems Security*

HIGH-LEVEL CONTROL OBJECTIVE

DS5 Deliver and Support

Ensure Systems Security



Control over the IT process of

ensuring systems security

that satisfies the business requirement

to safeguard information against unauthorised use, disclosure or modification, damage or loss

is enabled by

logical access controls that ensure that access to systems, data and program is restricted to authorised users

and takes into consideration

- Confidentiality and privacy requirements
- Authorisation, authentication and access control
- User identification and authorisation profiles
- Need-to-have and need-to-know
- Cryptographic key management
- Incident handling, reporting and follow-up
- Virus prevention and detection
- Firewalls
- Centralised security administration
- User training
- Tools for monitoring compliance, intrusion testing and reporting

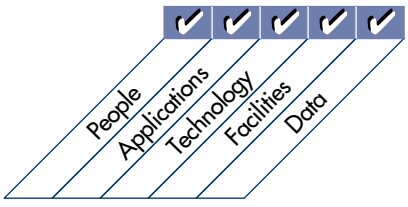


Figure 38—Control Objectives for *Ensure Systems Security (cont.)*

DETAILED CONTROL OBJECTIVES

5 ENSURE SYSTEMS SECURITY

5.1 Manage Security Measures

CONTROL OBJECTIVE

IT security should be managed such that security measures are in line with business requirements. This includes:

- Translating risk assessment information to the IT security plans
- Implementing the IT security plan
- Updating the IT security plan to reflect changes in the IT configuration
- Assessing the impact of change requests on IT security
- Monitoring the implementation of the IT security plan
- Aligning IT security procedures to other policies and procedures

5.2 Identification, Authentication and Access

CONTROL OBJECTIVE

The logical access to and use of IT computing resources should be restricted by the implementation of adequate identification, authentication and authorisation mechanisms, linking users and resources with access rules. Such mechanisms should prevent unauthorised personnel, dial-up connections and other system (network) entry ports from accessing computer resources and minimise the need for authorised users to use multiple sign-ons. Procedures should also be in place to keep authentication and access mechanisms effective (e.g., regular password changes).

5.3 Security of Online Access to Data

CONTROL OBJECTIVE

In an online IT environment, IT management should implement procedures in line with the security policy that provides access security control based on the individual's demonstrated need to view, add, change or delete data.

5.4 User Account Management

CONTROL OBJECTIVE

Management should establish procedures to ensure timely action relating to requesting, establishing, issuing, suspending and closing user accounts. A formal approval procedure outlining the data or system owner granting the access privileges should be included. The security of third-party access should be defined contractually and address administration and nondisclosure requirements. Outsourcing arrangements should address the risks, security controls and procedures for information systems and networks in the contract between the parties.

5.5 Management Review of User Accounts

CONTROL OBJECTIVE

Management should have a control process in place to review and confirm access rights periodically. Periodic comparison of resources with recorded accountability should be completed to help reduce the risk of errors, fraud, misuse or unauthorised alteration.

5.6 User Control of User Accounts

CONTROL OBJECTIVE

Users should systematically control the activity of their proper account(s). Information mechanisms should be in place to allow them to oversee normal activity as well as to be alerted to unusual activity in a timely manner.

5.7 Security Surveillance

CONTROL OBJECTIVE

IT security administration should ensure that security activity is logged, and any indication of imminent security violation is reported immediately to all who may be concerned (internally and externally) and acted upon in a timely manner.

continued on next page

Figure 38—Control Objectives for *Ensure Systems Security (cont.)*

5.8 **Data Classification**
CONTROL OBJECTIVE
Management should implement procedures to ensure that all data are classified in terms of sensitivity by a formal and explicit decision by the data owner according to the data classification scheme. Even data needing "no protection" should require a formal decision to be so designated. Owners should determine disposition and sharing of data, as well as whether and when programs and files are to be maintained, archived or deleted. Evidence of owner approval and data disposition should be maintained. Policies should be defined to support reclassification of information, based on changing sensitivities. The classification scheme should include criteria for managing exchanges of information between organisations, addressing both security and compliance with relevant legislation.

5.9 **Central Identification and Access Rights Management**
CONTROL OBJECTIVE
Controls are in place to ensure that the identification and access rights of users as well as the identity of system and data ownership are established and managed in a unique and central manner to obtain consistency and efficiency of global access control.

5.10 **Violation and Security Activity Reports**
CONTROL OBJECTIVE
IT security administration should ensure that violation and security activity is logged, reported, reviewed and appropriately escalated on a regular basis to identify and resolve incidents involving unauthorised activity. The logical access to the computer resources accountability information (security and other logs) should be granted based upon the principle of least privilege or on a need-to-know basis.

5.11 **Incident Handling**
CONTROL OBJECTIVE
Management should establish a computer security incident handling capability to address security incidents by providing a centralised platform with sufficient expertise and equipped with rapid and secure communication facilities. Incident management responsibilities and procedures should be established to ensure an appropriate, effective and timely response to security incidents.

5.12 **Reaccreditation**
CONTROL OBJECTIVE
Management should ensure that reaccreditation of security (e.g., through "tiger teams") is periodically performed to update the formally approved security level and the acceptance of residual risk.

5.13 **Counterparty Trust**
CONTROL OBJECTIVE
Organisational policy should ensure that control practices are implemented to verify the authenticity of the counterparty providing electronic instructions or transactions. This can be implemented through trusted exchange of passwords, tokens or cryptographic keys.

5.14 **Transaction Authorisation**
CONTROL OBJECTIVE
Organisational policy should ensure that, where appropriate, controls are implemented to provide authenticity of transactions and establish the validity of a user's claimed identity to the system. This requires use of cryptographic techniques for signing and verifying transactions.

Figure 38—Control Objectives for *Ensure Systems Security (cont.)*

5.15 **Nonrepudiation**
CONTROL OBJECTIVE
Organisational policy should ensure that, where appropriate, transactions cannot be denied by either party and controls are implemented to provide nonrepudiation of origin or receipt, proof of submission and receipt of transactions. This can be implemented through digital signatures, time stamping and trusted third parties, with appropriate policies that take into account relevant regulatory requirements.

5.16 **Trusted Path**
CONTROL OBJECTIVE
Organisational policy should ensure that sensitive transaction data are exchanged only over a trusted path. Sensitive information includes security management information, sensitive transaction data, passwords and cryptographic keys. To achieve this, trusted channels may need to be established using encryption between users, between users and systems, and between systems.

5.17 **Protection of Security Functions**
CONTROL OBJECTIVE
Security-related hardware and software should at all times be protected against tampering and against disclosure of secret keys to maintain their integrity. In addition, organisations should keep a low profile about their security design, but should not base their security on the design being secret.

5.18 **Cryptographic Key Management**
CONTROL OBJECTIVE
Management should define and implement procedures and protocols to be used for 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. If a key is compromised, management should ensure that this information is propagated to any interested party through the use of certificate revocation lists or similar mechanisms.

5.19 **Malicious Software Prevention, Detection and Correction**
CONTROL OBJECTIVE
Regarding malicious software, such as computer viruses or Trojan horses, management should establish a framework of adequate preventive, detective and corrective control measures, and occurrence response and reporting. Business and IT management should ensure that procedures are established across the organisation to protect information systems and technology from computer viruses. Procedures should incorporate virus protection, detection, occurrence response and reporting.

5.20 **Firewall Architectures and Connections with Public Networks**
CONTROL OBJECTIVE
If connection to the Internet or other public networks exists, adequate firewalls should be operative to protect against denial of services, unauthorised access to the internal resources and control any application and infrastructure management flows in both directions.

5.21 **Protection of Electronic Value**
CONTROL OBJECTIVE
Management should protect the continued integrity of all cards or similar physical mechanisms used for authentication or storage of financial or other sensitive information, taking into consideration the related facilities, devices, employees and validation methods used.

Figure 39—Control Practices for *Ensure Systems Security*

DS5.1 Manage Security Measures

Why Do It?

Adequate management of security measures will help:

- Ensure that security strategy provides solutions for the real business challenges or needs
- Ensure synchronisation of the security strategy with the overall business plan
- Avoid exposure of the organisation to new vulnerabilities
- Ensure that all implications are considered and the latest technology evolution is taken into account
- Establish targets for which progress can be measured
- Ensure that appropriate security is implemented and maintained
- Ensure that security requirements, objectives, policies, standards and procedures are consistent with applicable laws and regulations
- Ensure that individual security responsibilities are clearly defined
- Ensure that employees have the required knowledge of the organisation's security-related policies and procedures as well as the appropriate security-minded attitude
- Ensure that asset ownership is established

Control Practices

1. The need to prepare and maintain a technological strategic and tactical security plan are laid out in a policy.
2. The responsibility for the preparation, maintenance and approval of such strategic and tactical security plans (including succession plans) is identified, and the required skills for this task are available within the organisation. Senior management from across the organisation is involved.
3. Independent advice (internal or external) and comment on the security plan are solicited prior to the plan's implementation.
4. The security strategy is linked into the organisation's overall operating plan/strategy, security policy, security standards and security practices/guidelines. Management challenges and reviews the strategy periodically and ensures that it remains in line with the strategic business plan.
5. The security strategy specifies the path to the desired level of security in measurable terms by relating progress to benchmarks.
6. The security strategy has metrics that are benchmarked against industry scores. Independent reviewers validate metrics scores.
7. The security strategy is based on a formal risk analysis, taking into account that risk has many different components: assets, threats, vulnerabilities, safeguards, consequences and likelihood.
8. Detailed plans are formulated and documented to implement the security strategy, resulting in the development and implementation of a better computer security programme and in the better protection of systems and information.
9. Security requirements, objectives, policies, standards and procedures are identified, documented and published.
10. Documented security requirements, objectives, policies, standards and procedures are consistent with applicable laws and regulations and with contractual, legal and other service level agreements.
11. A process for communicating the strategy, plans, policies and procedures exists, ensuring that the policy has visibility and clear mandates, and roles and responsibilities are defined and updated as the environment changes.
12. Senior management refers to the security strategy and encourages staff to do so.
13. The security responsibilities of managers and employees at all levels are clearly defined in their job descriptions, and they are qualified to fulfil their responsibilities.
14. Security awareness, including data ownership responsibilities and virus protection requirements, is part of the employee orientation programme, education and training programme and performance appraisal process.
15. A management framework is established to initiate and control the implementation of information security within the organisation. The corporate security function reports to senior management and is held accountable for executing the security plan.
16. A management approval process for new IT facilities is established to ensure that the installation of equipment is for a defined business purpose, provides an adequate level of security protection and does not adversely affect the security of the existing infrastructure.
17. Information security advisors or focal points are established and are equipped to provide advice on all aspects of information security. They are allowed direct access to IT and business managers throughout the organisation.
18. The actual practice of information security is reviewed independently to provide assurance that organisational practices properly reflect the policy and are feasible and effective.
19. Guidelines for allocation of ownership responsibilities are established and included in policy statements. Roles and responsibilities of owners are defined.
20. Trends and technology developments are monitored to ensure cost-effective and competitively advantageous use of security technology and to prevent obsolescence.
21. Third-party evaluation of security policy and architecture is conducted periodically.

Figure 39—Control Practices for *Ensure Systems Security (cont.)*

DS5.2 Identification, Authentication and Access

Why Do It?
Controlling identification, authentication and access in line with the control practices will help ensure that:
- External users are confident that the system is adequately secure
- Systems and information are protected to prevent unauthorised access or use
- Minimum security requirements are specified for all system components
- Authentication and access mechanisms remain effective
- Appropriate segregation exists amongst production, test and development environments
- Personnel are informed of management's rights to monitor and inspect all usage of information technology resources, including e-mail, voice communications, and all programs and data files
- Proper investigation is conducted for all access activity that is not compliant with the organisation's established policies and procedures

Control Practices
1. Policies are in place to ensure that the owners of a system with external users have the responsibility to share appropriate knowledge about the existence and general extent of security measures, so those external users can be confident that the system is adequately secure.
2. Systems and information are protected to prevent unauthorised access or use.
3. Minimum security requirements are specified for all operating systems and versions deployed in the organisation. Operating systems are tested to comply with these minimum requirements and tailored where necessary. Compliant operating system versions, e.g., operating system security parameters based on vendor/organisational standards, are installed on all systems. Deviations are formally approved after assessment of compensating controls.
4. Minimum security requirements are specified for all system components, e.g., software, hardware and communications equipment, and such security is an integral part of the organisation's SDLC.
5. Compliance with security baselines is reviewed regularly.
6. Logical access to computing resources is restricted by implementation of adequate authentication mechanisms for identified users.
7. Resources are protected by access rules based on adequate identification and authentication of resource users.
8. A single sign-on is required for all required resources.
9. Procedures are in place to keep authentication and access mechanisms effective.
10. Following a system failure, users are not allowed back on the system without reauthentication.
11. The granting of access, changes to existing access rights and removal of access is authorised by the appropriate system owner, taking into account least privilege, segregation of duties and the level of access required.
12. Business users are not granted access to development and test systems except where specifically required for user testing.
13. The definition of emergency situations and the action that must be taken is provided by the asset owner, ensuring that individuals to whom emergency access rights can be given are nominated in advance, emergency rights are removed as soon as the emergency is resolved, and all actions are logged.
14. Terminals that, for technical or business reasons, are protected only by restricting access to the room in which they are located are physically identified and authenticated by their host computer systems before access is granted.
15. All systems require a user identifier and user authentication mechanism to allow access.
16. Systems validate the user identifier and user authenticator combination as a pair and reject the logon attempt if it is invalid. Systems do not inform the user which of the two is wrong.
17. Arrangements involving third-party access to organisational IT facilities are based on a formal contract containing or referring to all of the necessary security conditions to ensure compliance with the organisation's security policies and standards.
18. Access to diagnostic ports is controlled by an appropriate security mechanism, e.g., a key lock and a procedure, to ensure that these ports are accessible only through arrangements between accountable officials and support personnel.
19. Personnel are advised that management reserves the right to monitor and inspect all usage of information technology resources, including e-mail, voice communications, and all programs and data files. It should be stressed that this is done to protect privacy and the rights and interests of others.
20. All access activity that is not compliant with the organisation's established policies and procedures is investigated.

Figure 39—Control Practices for *Ensure Systems Security (cont.)*

21. Strong user identification techniques, such as dynamic passwords, challenge response, biometrics and/or public key cryptography, are used to protect the organisation's IT resources from inappropriate access by individuals outside the organisation.

DS5.3 Security of Online Access to Data

Why Do It?
Proper implementation of security of online access to data in line with the control practices will ensure that:
- Access to data is granted on a need-to-know basis
- Appropriate segregation exists amongst production, test and development environments

Control Practices
1. Access to data is granted on a need-to-know basis.
2. Strict controls are maintained over access to production libraries.
3. Production source libraries are updated only via a formal change process by designated staff with change control responsibilities.
4. Key security parameters and processes are identified and their content is periodically compared to a protected baseline of authorised contents.

DS5.4 User Account Management

Why Do It?
The enforcement of adequate user account management in line with the control practices will help ensure that:
- The life cycle of user accounts is properly administrated
- Users are informed of the rules and acknowledge those rules with which they need to comply

Control Practices
1. Procedures are in place to ensure timely actions in relation to requesting, establishing, issuing, suspending and closing user accounts. All actions require formal approval.
2. When employees are given their account, they are provided with initial or refresher training and awareness on computer security issues. Users are asked to review a set of rules and regulations for system access.
3. Users use quality passwords as determined by the organisation's password guidelines. Quality aspects of passwords include enforcement of initial password change on first use, appropriate minimum password length, appropriate and enforced frequency of password changes, password checking against a list of not-allowed values, and adequate protection of emergency passwords.
4. Third-party users are not provided with user codes or passwords unless they have signed a nondisclosure agreement. Third-party users are granted access to the organisation's security policy and related documents and must confirm that they understand their obligations.
5. All contracts for outsourcing or contracting address the need for the provider to comply with all security-related policies, standards and procedures.

DS5.5 Management Review of User Accounts

Why Do It?
The appropriate organisation of management review of user accounts in line with the control practices will:
- Ensure that unauthorised changes to access rights are detected in a timely manner

Control Practice
1. Access rights are reviewed periodically to confirm that they are still as granted and they correspond to the user's and the organisation's needs.

DS5.6 User Control of User Accounts

Why Do It?
Appropriate user control of user accounts in line with the control practices will help ensure that:
- Abnormal activity, typically usage of accounts after hours or during holidays/sickness, is detected in a timely manner and reported promptly for formal investigation

Control Practice
1. Users control the activity of their accounts by reviewing login times. Any abnormal activity is reported in a timely manner.

DS5.7 Security Surveillance

Why Do It?
The implementation of security surveillance in line with the control practices will help:
- Recognise attack patterns based on historical data
- Effective and efficient investigation of security breaches
- Ensure that security logs are a reliable source of information for investigation of security breaches

Figure 39—Control Practices for *Ensure Systems Security (cont.)*

Control Practices
1. The organisation has a centralised system to allow reporting of security breaches, and the investigative actions are summarised in a log. The importance of the reported items is assessed, appropriately escalated and investigated.
2. Specific security events that require examination and possible investigation are identified and included on the audit trail with appropriate information needed to support problem resolution.
3. No user access to security logs is allowed. Only programs known to have valid reasons for writing audit records are allowed to amend audit log files.
4. A process is defined to have appropriate security personnel determine whether failed access attempts were genuine mistakes or deliberate attempts to perform an unauthorised function.
5. Audit trails are retained for at least six months, unless otherwise required by legal, regulatory or any other business needs.
6. Automated systems or manual processes are deployed and acted upon to ensure that any imminent security violation is reported immediately to all who may be concerned, internally and externally.

DS5.8 Data Classification

Why Do It?
Requiring data classification in line with the control practices will help:
- Establish clear security requirements and ensure that the appropriateness of the level of security is verifiable
- Ensure that data are classified and labelled accordingly
- Ensure that data and system owners have the authority to enforce the protection of assets required by the classification

Control Practices
1. There is a clearly articulated process for establishing an owner for each information technology component in the organisation.
2. Responsibilities of data owners are formalised. At a minimum, owners determine disposition and sharing of data (within the organisation or with third parties), as well as whether and when programs and files are to be maintained, archived or deleted.
3. All data are classified in terms of sensitivity through a formal and explicit decision made by the data owner according to the data classification scheme.
4. Reclassification of information based on changing sensitivities is supported by the policies and procedures for data classification.
5. Tools are available to help data owners determine the classification of their data security.
6. Owners have sufficient authority and knowledge to understand the value of the assets they own and balance security needs against cost considerations and other business requirements.
7. Where an asset has been assessed as having a certain classification, any component inherits the same classification.
8. Protection requirements from inception through destruction for each data and system classification scheme are identified.
9. Classified information and outputs from systems handling organisationally classified data are labelled appropriately.

DS5.9 Central Identification and Access Rights Management

Why Do It?
Implementation of central identification and access rights management in line with the control practices will help ensure that:
- Security profiles assigned by the multiple security or system administrators involved are consistent

Control Practices
1. System access is centrally managed to ensure consistent user profiles for all systems.
2. Users are identified and assigned authorisations in a standard and efficient manner, preferably using a centralised user management process and system.

DS5.10 Violation and Security Activity Reports

Why Do It?
The design and implementation of violation and security activity reports in line with the control practices will help ensure that:
- System abuse and security violations cannot go undetected and security breaches cannot continue for a prolonged period of time.

Control Practice
1. Security-related activity is logged. Security logs are reviewed and exceptions followed up to find root causes. Appropriate reporting and escalation are in place.

Figure 39—Control Practices for *Ensure Systems Security (cont.)*

DS5.11 Incident Handling

Why Do It?
Enforcing formal incident handling in line with the control practices will help ensure that:
- Sufficient expertise is available for the review of security breaches
- Up-to-date information is available to effectively counteract identified attacks
- Management is made aware of the number, frequency and importance of security breaches

Control Practices
1. Reported security incidents (breaches) are reviewed promptly by a central team with sufficient expertise to minimise damage and find/eliminate the root cause for the security breach.
2. Management is informed of all significant security breaches.
3. There is an adequately communicated formal disciplinary process for employees who are found to have violated organisational security policies and procedures; employees and contractors are made aware of this process.

DS5.12 Reaccreditation

Why Do It?
The existence of adequate procedures for reaccreditation in line with the control practices will help ensure that:
- The implemented security controls remain up-to-date as hackers find new ways to breach implemented controls
- Discrepancies between the requirements prescribed by the security design and the implemented security controls are noticed in a timely manner

Control Practice
1. The security design and implemented security controls are regularly reviewed to ensure that the implementation corresponds to the architecture and the architecture is kept up to date with advances in security technology.

DS5.13 Counterparty Trust

Why Do It?
The existence of adequate procedures to maintain counterparty trust in line with the control practices will help:
- Avoid certified identities from being assigned to hackers or unauthorised users

Control Practices
1. A registration authority, functioning as a trusted third party, verifies the credentials of a connecting party before transactions can be exchanged.
2. A certification authority certifies a registered party to ensure counterparty trust.

DS5.14 Transaction Authorisation

Why Do It?
Implementing controls over transaction authorisation in line with the control practices will ensure that:
- The organisation has the capability to verify that business transactions have been originated by authorised individuals or devices
- Processes do not accept any message that is offered for processing as a genuine business transaction unless the transaction has been digitally signed and the signature has been successfully verified

Control Practices
1. Cryptographic techniques are used for signing transactions and verifying signatures to confirm the integrity of the transaction.
2. The validity of a user's claimed identity to the system is established.

DS5.15 Nonrepudiation

Why Do It?
Implementing controls over transaction authorisation in line with the control practices will ensure that:
- Transactions accepted for processing have been originated by authorised individuals or devices

Control Practices
1. Where required, digital signatures are applied to ensure that data were transmitted by a known source.
2. Time stamps are added to transactions and included in the message content that is subject to signature. Time stamps are based on synchronised clocks and take into account times zones where appropriate.

Figure 39—Control Practices for *Ensure Systems Security (cont.)*

DS5.16 Trusted Path

Why Do It?
The existence of trusted paths for business communication in line with the control practices will ensure that:
- Sensitive information cannot be exposed to unauthorised parties
- Proper physical security is in place to guarantee the security of media

Control Practice
1. Sensitive data, e.g., keys, security management information, confidential data and passwords, are exchanged only over a secure path. This requires encryption as well as appropriate physical protection of the carrier, where possible.

DS5.17 Protection Security Functions

Why Do It?
Providing appropriate protection of security functions in line with the control practices will:
- Avoid the exposure of such information to unauthorised individuals
- Help maintain the existing trust relationship with other organisations

Control Practices
1. All hardware related to the security function is tamperproof, and guarantees exist that secret keys cannot be exposed.
2. The security design is confidential, but strong enough to resist exposure, in case it is made available to unauthorised individuals.

DS5.18 Cryptographic Key Management

Why Do It?
Appropriate cryptographic key management in line with the control practices will:
- Ensure that cryptographic keys have not been shared with malicious parties
- Guarantee that registered users' credentials have been successfully verified
- Ensure that only authorised users have access to cryptographic keys

Control Practices
1. 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.
2. A proper ceremony with witnesses is held for the generation or renewal of root keys.
3. Procedures are in place to determine when root key renewal is required.
4. A certification practices statement (CPS) is written. The CPS describes the certificate practices that have been implemented in the certification authority (CA), registration authority (RA) and directory to comply with the policies for the handling of the various certificate classes as defined in the certificate policy documents. The CPS version is mentioned in each certificate issued.
5. Cryptographic keys are generated by a trusted third party, after appropriate verification of the requester's credentials (registration authority).
6. Cryptographic keys are distributed using secure offline mechanisms.
7. Certification is required before a secure communication channel, using the cryptographic keys, can be set up.
8. Keys are stored in encrypted form, regardless of the storage medium used.
9. Compromised keys are revoked as soon as possible and all parties concerned are informed of the revocation.

DS5.19 Malicious Software Prevention, Detection and Correction

Why Do It?
Implementing adequate malicious software prevention, detection and correction in line with the control practices will:
- Ensure the availability and integrity of systems and data, and potentially ensure that the confidentiality of the data is safeguarded against virus attacks
- Ensure that information on new security threats is gathered and reviewed by the central security team, allowing recognition of new types of attacks and updating of defence systems to counter new types of attacks
- Avoid the unauthorised customisation of software or installation of unapproved software
- Avoid the use of illegal software or unsupported versions of legal software
- Ensure that the organisation has proper means to demonstrate compliance with licence agreements

Figure 39—Control Practices for *Ensure Systems Security (cont.)*

Control Practices

1. Virus protection is active, and virus definition files are kept up to date.
2. All executable code is scanned for viruses before introduction into the internal network.
3. Procedures for escalation, damage containment and recovery in the event of a computer virus occurrence are defined, documented and communicated.
4. Information on new security threats is reviewed.
5. Software is distributed centrally and version and patch-level controls are implemented using centralised configuration management.
6. Unauthorised changes to software, changes that have not gone through the normal development cycle and/or the installation of unapproved software are prohibited.
7. Computing platforms are reviewed for unauthorised software.
8. Only licenced copies of software are installed. Software usage is limited to the allowed number of concurrent users.
9. Copying licenced software owned by the organisation, for personal or nonbusiness-related use, is prohibited.
10. All incidents are kept in a central log and tracked until closure. Management reporting is in place on the number and severity as well as the closure time for such issues.

DS5.20 Firewall Architectures and Connections With Public Networks

Why Do It?

Implementing adequate firewall architectures and connections with public networks in line with the control practices will:

- Ensure that unauthorised attempts to access information over the network are prevented and detected
- Ensure that there is no possibility to bypass the firewall
- Ensure that the firewall's configuration is in line with the organisation's security policy
- Avoid unauthorised inspection or modification of the firewall rule base
- Ensure proper segregation of networks with different security classifications

Control Practices

1. The organisation's firewall policy is reviewed/audited and updated at least twice per year (preferably quarterly). A formal process is used for managing the addition and deletion of firewall rules. In addition, firewall penetration analyses are performed periodically, if Internet connectivity is employed.
2. A firewall is installed, and all traffic is forced to pass through it.
3. Only authorised traffic, as defined by the local security policy, is allowed to pass. The firewall default policy for handling inbound traffic blocks all packets and connections unless the traffic type and connections are permitted specifically (as opposed to permitting all connections and traffic by default and then blocking specific traffic and connections).
4. All network traffic relating to firewall system management is secured properly.
5. The firewall itself is immune to penetration. The firewall architecture protects itself from attack through active monitoring and pattern recognition.
6. The firewall architecture combines protection measures at the application and network level. An in-depth defence is created by implementing layers of security, as opposed to allowing a firewall to serve as the single/only security layer (e.g., use of a boundary router or separate firewall at the Internet connection to create an external DMZ for web servers and other publicly accessible servers, whilst using a second firewall to protect internal networks/users).
7. Firewall platforms are implemented on systems containing operating system builds with minimal feature sets (i.e., those that have been stripped of all unnecessary functionality and hardened for security applications, thereby becoming, in effect, a bastion host); firewalls are never placed on systems built with all possible installation options. In addition, all operating system patches are applied in a timely manner.
8. Traffic is exchanged through the firewall only at the application layer.
9. The firewall architecture enforces protocol discontinuity at the transport layer.
10. Strong authentication is used for the management of the firewall.
11. The firewall hides the structure of the organisation's internal network.
12. The firewall provides an audit trail of all communications to or through the firewall system and generates alarms when suspicious activity is detected.
13. Hosts connected to public networks are located outside the firewall.
14. Subnetworks that carry data of different sensitivity levels are segregated.
15. The organisation's firewall environment is covered by its disaster recovery/continuity-of-operations plan.
16. All firewalls are subject to a day-zero backup—backed up immediately prior to production releases, subjected to full rather than incremental backups and employ an internally situated backup mechanism (e.g., tape drive). Firewall

Figure 39—Control Practices for *Ensure Systems Security (cont.)*

backups are not written to any backup servers located on unprotected networks to avoid opening a potential security hole to that network.

DS5.21 Protection of Electronic Value

Why Do It?
Implementing adequate protection of electronic value in line with the control practices will help ensure:
• Confidentiality, availability and integrity of information

Control Practices
1. The integrity of all data is guaranteed by controlling changes through the use of access control mechanisms as well as monitoring for unauthorised changes.
2. Adequate physical security protects authentication devices and storage/processing facilities.

Figure 40—Audit Guidelines for *Ensure Systems Security*

DS5 Ensure Systems Security

Control Objectives	
1	Manage security measures
2	Identification, authentication and access
3	Security of online access to data
4	User account management
5	Management review of user accounts
6	User control of user accounts
7	Security surveillance
8	Data classification
9	Central identification and access rights management
10	Violation and security activity reports
11	Incident handling
12	Reaccreditation
13	Counterparty trust
14	Transaction authorisation
15	Nonrepudiation
16	Trusted path
17	Protection of security functions
18	Cryptographic key management
19	Malicious software prevention, detection and correction
20	Firewall architectures and connections with public networks
21	Protection of electronic value

BOTH HIGH-LEVEL AND DETAILED CONTROL OBJECTIVES ARE AUDITED BY:

Obtaining an understanding by:

- **Interviewing:**

  Senior security officer of the organisation
  IT senior and security management
  IT database administrator
  IT security administrator
  IT application development management

- **Obtaining:**

  Organisationwide policies and procedures relating to information system security and access
  IT policies and procedures relating to information systems security and access
  Relevant policies, procedures, and legal and regulatory body information systems security requirements (i.e., laws, regulations, guidelines, industry standards) including:
  - User account management procedures

Figure 40—Audit Guidelines for *Ensure Systems Security (cont.)*

- User security or information protection policy
- Standards regarding electronic commerce
- Data classification schema
- Inventory of access control software
- Floor plan of buildings/rooms housing IT resources
- Inventory or schematic of physical access points to IT resources (i.e., modems, telephone lines and remote terminals)
- Security software change control procedures
- Problem tracking, resolution and escalation procedures
- Security violation reports and management review procedures
- Inventory of data encryption devices and encryption standards
- List of vendors and customers with access to system resources
- List of service providers used in transmission of data
- Network management practices regarding continuous security testing
- Copies of contracts with service providers for data transmission
- Copies of signed user security and awareness documents
- Content of new employee training materials relating to security
- Audit reports from external auditors, third-party service providers and governmental agencies related to information system security

Evaluating the controls by:

► **Considering whether:**

The strategic security plan is in place providing centralised direction and control over information system security, along with user security requirements for consistency

A centralised security organisation is in place responsible for ensuring only appropriate access to system resources

Data classification schema are in place and being used and all system resources have an owner responsible for security and content

User security profiles are in place representing “least access as required” and profiles are regularly reviewed by management for reaccreditation

Employee indoctrination includes security awareness, ownership responsibility and virus protection requirements

Reporting exists for security breaches, and formal problem resolution procedures are in place and these reports include:

- Unauthorised attempts to access system (sign-on)
- Unauthorised attempts to access system resources
- Unauthorised attempts to view or change security definitions and rules
- Resource access privileges by user ID
- Authorised security definitions and rule changes
- Authorised access to resources (selected by user or resource)
- Status change of the system security
- Accesses to operating system security parameter tables

Cryptographic modules and key maintenance procedures exist, are administered centrally, and are used for all external access and transmission activity

Cryptographic key management standards exist for both centralised and user activity

Change control over security software is formal and consistent with normal standards of system development and maintenance

Figure 40—Audit Guidelines for *Ensure Systems Security (cont.)*

The authentication mechanisms in use provide one or more of the following features:
- Single use of authentication data (e.g., passwords are never reusable)
- Multiple authentication (i.e., two or more different authentication mechanisms are used)
- Policy-based authentication (i.e., ability to specify separate authentication procedures for specific events)
- On-demand authentication (i.e., ability to reauthenticate the user at times after the initial authentication)

The number of concurrent sessions belonging to the same user is limited

At logon, an advisory warning message is sent to users regarding the appropriate use of hardware, software or the logon connection

A warning screen is displayed prior to completing logon to inform reader that unauthorised access may result in prosecution

Upon successful session establishment, a history of successful and unsuccessful attempts to access the user's account is displayed to the user

Password policy includes:
- Enforcement of initial password change on first use
- An appropriate minimum password length
- An appropriate and enforced frequency of password changes
- Password checking against list of not-allowed values (e.g., dictionary checking)
- Adequate protection of emergency passwords

Formal problem resolution procedures include:
- User ID is suspended after five repeated unsuccessful logon attempts
- Date, time of last access and number of unsuccessful attempts are displayed to authorised user at logon
- Authentication time is limited to five minutes, after which the session is terminated
- User is informed of suspension, but not the reason for it

Dial-in procedures include dial-back or token-based authentication, frequent changes of dial-up numbers, software and hardware firewalls to restrict access to assets, and frequent changes of passwords and deactivation of former employees' passwords

Location control methods are used to apply additional restrictions at specific locations

Access to the voicemail service and the PBX system are controlled with the same physical and logical controls as for computer systems

Enforcement of sensitive position policies occurs, including:
- Employees in sensitive job positions are required to be away from the organisation for an appropriate period of time every calendar year; during this time their user ID is suspended and persons replacing the employee are instructed to notify management if any security-related abnormalities are noted.
- Unannounced rotation of personnel involved in sensitive activities is performed from time to time.

Security-related hardware and software, such as cryptographic modules, are protected against tampering or disclosure, and access is limited to a need-to-know basis

Access to security data such as security management, sensitive transaction data, passwords and cryptographic keys is limited to a need-to-know basis

Trusted paths are used to transmit nonencrypted sensitive information

To prevent denial of service due to an attack with junk faxes, protective measures are taken such as:
- Limiting the disclosure of fax numbers outside the organisation to a need-to-know basis
- Fax lines used for solicitation of business are not used for other purposes

Preventive and detective control measures have been established by management with respect to computer viruses

To enforce integrity of electronic value, measures are taken such as:
- Card reader facilities are protected against destruction, disclosure or modification of the card information
- Card information (PIN and other information) is protected against insider disclosure
- Counterfeiting of cards is prevented

To enforce protection of security features, measures are taken such as:
- The identification and authentication process is required to be repeated after a specified period of inactivity
- A one-button lock-up system, a force button or a shut-off sequence can be activated when the terminal is left alone

Figure 40—Audit Guidelines for *Ensure Systems Security (cont.)*

Assessing the compliance by:

► **Testing that:**

The IT function is in compliance with security standards relating to:

- Authentication and access
- Managing user profiles and data security classifications
- Violation and security incident reporting and management review
- Cryptographic key management standards
- Virus detection, resolution and communication
- Data classification and ownership

Procedures for requesting, establishing and maintaining user access to system exist

Procedures for external access to system resources (i.e., logon, ID, password, dial-back) exist

Inventory of access devices for completeness is maintained

Operating system security parameters are based on vendor/local standards

Network security management practices are communicated, understood and enforced

External access provider contracts include consideration of security responsibilities and procedures

Actual logon procedures for systems, users and external vendor access exist

Security reporting is occurring for timeliness, accuracy and management response to incidents

Secret keys exist for transmission utilisation

Procedures for protection from malicious software include:

- All software acquired by the organisation is checked for viruses prior to installation and use.
- A written policy exists on downloading, acceptance and use of freeware and shareware, and this policy is adhered to.
- Software for highly critical applications is protected by message authentication code (MAC) or digital signature, and a failure to verify prevents the software from being used.
- Users have received instructions on the detection and reporting of viruses, as indicated by such phenomena as sluggish performance or mysterious growth of files.
- A policy and procedure exist and are adhered to for the checking of diskettes brought in from outside the organisation's normal purchasing programme.

Firewalls have at least the following properties:

- All traffic from inside to outside, and *vice versa*, must pass through the firewall (this should not be limited to logical controls, but should also be physically enforced).
- Only authorised traffic, as defined by local security policy, is allowed to pass.
- The firewall itself is immune to penetration.
- Traffic is exchanged through the firewall at the application layer only.
- The firewall architecture combines control measures at the application and network level.
- The firewall architecture enforces a protocol discontinuity at the transportation layer.
- The firewall architecture should be configured according to the "minimal art philosophy."
- The firewall architecture should deploy strong authentication for management of its components.
- The firewall architecture hides the structure of the internal network.
- The firewall architecture provides an audit trail of all communications to or through the firewall system and generates alarms when suspicious activity is detected.
- Organisation's hosts, which provide support for incoming service requests from the public network, are sitting outside the firewall.
- The firewall architecture defends itself from direct attack (e.g., through active monitoring of traffic and pattern recognition technology).

Figure 40—Audit Guidelines for *Ensure Systems Security (cont.)*

- All executable code is scanned for malicious code (e.g., viruses, malicious applets) before it is introduced to the internal network.

Substantiating the risk of control objectives not being met by:

► **Performing:**

Benchmarking of information system security against similar organisations or appropriate international standards/recognised industry best practices

A detailed review of information system security, including penetration evaluations of physical and logical security of computer and communications resources, etc.

An interview of new employees to ascertain awareness of security and individual responsibilities (i.e., confirm signed security statements and new employee training regarding security)

An interview of users to ascertain that access is determined on a business need ("least needed") and reviewed regularly by management for accuracy

► **Identifying:**

Inappropriate user access to system resources

Inconsistencies with network schematic or inventory relating to missing access points, missing accessories, etc.

Contract deficiencies relating to ownership and responsibilities relating to data integrity and security at any point in transmission between send and receipt

Employees not verified as legitimate users or former employees that still have access

Informal or unapproved requests for access to system resources

Network monitoring software that does not alert network management of security breaches

Shortcomings of network software change control procedures

Non-use of secret keys in third-party submission/receipt procedures

Deficiencies in protocols for key generation, distribution, storage, entry, use, archiving and protection

Noncurrent virus detection software or lack of formal procedures for preventing, detecting, correcting and reporting infestations

Figure 41—Management Guidelines for *Ensure Systems Security*

DS5 Deliver and Support
Ensure Systems Security

Control over the IT process ***ensure systems security*** with the business goal of safeguarding information against unauthorised use, disclosure or modification, damage or loss

ensures delivery of information to the business that addresses the required information criteria and is measured by key goal indicators

is enabled by logical access controls that ensure that access to the systems, data and programs is restricted to authorised users

considers critical success factors that leverage specific IT resources and is measured by key performance indicators

Information Criteria	
	Effectiveness
	Efficiency
P	Confidentiality
P	Integrity
S	Availability
S	Compliance
S	Reliability

(**P**) primary (**S**) secondary

IT Resources
✓ People
✓ Applications
✓ Technology
✓ Facilities
✓ Data

(✓) applicable to

Critical Success Factors

- An overall security plan is developed that covers building awareness, establishes clear policies and standards, identifies a cost-effective and sustainable implementation, and defines monitoring and enforcement processes.
- There is awareness that a good security plan takes time to evolve.
- The corporate security function reports to senior management and is responsible for executing the security plan.
- Management and staff have a common understanding of security requirements, vulnerabilities and threats, and they understand and accept their own security responsibilities.
- A third-party evaluation of security policy and architecture is conducted periodically.
- A "building permit" programme is defined, identifying security baselines that have to be adhered to.
- A "drivers licence" programme is in place for those developing, implementing and using systems, enforcing security certification of staff.
- The security function has the means and ability to detect, record, analyse significance, report and act upon security incidents when they do occur, while minimising the probability of occurrence by applying intrusion testing and active monitoring.
- A centralised user management process and system provide the means to identify and assign authorisations to users in a standard and efficient manner.
- A process is in place to authenticate users at reasonable cost, and is light to implement and easy to use.

Key Goal Indicators

- No incidents causing public embarrassment
- Immediate reporting on critical incidents
- Alignment of access rights with organisational responsibilities
- Reduced number of new implementations delayed by security concerns
- Full compliance, or agreed and recorded deviations from minimum security requirements
- Reduced number of incidents involving unauthorised access, loss or corruption of information

Key Performance Indicators

- Reduced number of security-related service calls, change requests and fixes
- Amount of downtime caused by security incidents
- Reduced turnaround time for security administration requests
- Number of systems subject to an intrusion detection process
- Number of systems with active monitoring capabilities
- Reduced time to investigate security incidents
- Time lag between detection, reporting and acting upon security incidents
- Number of IT security awareness training days

Figure 41—Management Guidelines for *Ensure Systems Security (cont.)*

DS5 Maturity Model

Control over the IT process ***ensure systems security*** with the business goal of safeguarding information against unauthorised use, disclosure or modification, damage or loss

0 **Nonexistent**—The organisation does not recognise the need for IT security. Responsibilities and accountabilities are not assigned for ensuring security. Measures supporting the management of IT security are not implemented. There is no IT security reporting and no response process to IT security breaches. There is a complete lack of a recognisable system security administration process.

1 **Initial/*Ad Hoc***—The organisation recognises the need for IT security, but security awareness depends on the individual. IT security is addressed on a reactive basis and not measured. IT security breaches invoke "finger pointing" responses if detected, because responsibilities are unclear. Responses to IT security breaches are unpredictable.

2 **Repeatable but Intuitive**—Responsibilities and accountabilities for IT security are assigned to an IT security co-ordinator with no management authority. Security awareness is fragmented and limited. IT security information is generated, but is not analysed. Security solutions tend to respond reactively to IT security incidents and by adopting third-party offerings, without addressing the specific needs of the organisation. Security policies are being developed, but inadequate skills and tools are still being used. IT security reporting is incomplete, misleading or not pertinent.

3 **Defined Process**—Security awareness exists and is promoted by management. Security awareness briefings have been standardised and formalised. IT security procedures are defined and fit into a structure for security policies and procedures. Responsibilities for IT security are assigned, but not consistently enforced. An IT security plan exists, driving risk analysis and security solutions. IT security reporting is IT-focused, rather than business-focused. *Ad hoc* intrusion testing is performed.

4 **Managed and Measurable**—Responsibilities for IT security are clearly assigned, managed and enforced. IT security risk and impact analysis is consistently performed. Security policies and practices are completed with specific security baselines. Security awareness briefings have become mandatory. User identification, authentication and authorisation are being standardised. Security certification of staff is being established. Intrusion testing is a standard and formalised process leading to improvements. Cost/benefit analysis, supporting the implementation of security measures, is increasingly being utilised. IT security processes are co-ordinated with the overall organisation security function. IT security reporting is linked to business objectives.

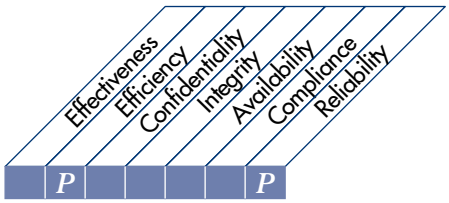
5 **Optimised**—IT security is a joint responsibility of business and IT management and is integrated with corporate security business objectives. IT security requirements are clearly defined, optimised and included in a verified security plan. Security functions are integrated with applications at the design stage and end users are increasingly accountable for managing security. IT security reporting provides early warning of changing and emerging risk, using automated active monitoring approaches for critical systems. Incidents are promptly addressed with formalised incident response procedures supported by automated tools. Periodic security assessments evaluate the effectiveness of implementation of the security plan. Information on new threats and vulnerabilities is systematically collected and analysed, and adequate mitigating controls are promptly communicated and implemented. Intrusion testing, root cause analysis of security incidents and proactive identification of risk is the basis for continuous improvements. Security processes and technologies are integrated organisationwide.

Figure 42—Control Objectives for *Identify and Allocate Costs*

HIGH-LEVEL CONTROL OBJECTIVE

DS6 Deliver and Support

Identify and Allocate Costs



Control over the IT process of

identifying and allocating costs

that satisfies the business requirement

to ensure a correct awareness of the costs attributable to IT services

is enabled by

a cost accounting system that ensures that costs are recorded, calculated and allocated to the required level of detail and to the appropriate service offering

and takes into consideration

- Resources identifiable and measurable
- Charging policies and procedures
- Charge rates and chargeback process
- Linkage to service level agreement
- Automated reporting
- Verification of benefit realisation
- External benchmarking

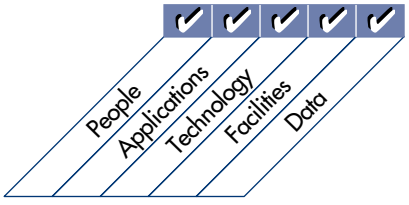


Figure 42—Control Objectives for *Identify and Allocate Costs (cont.)*

DETAILED CONTROL OBJECTIVES

6 IDENTIFY AND ALLOCATE COSTS

6.1 Chargeable Items

CONTROL OBJECTIVE

IT management, with guidance from senior management, should ensure that chargeable items are identifiable, measurable and predictable by users. Users should be able to control the use of information services and associated billing levels.

6.2 Costing Procedures

CONTROL OBJECTIVE

IT management should define and implement costing procedures to provide management information on the costs of delivering information services whilst ensuring cost-effectiveness. Variances between forecasts and actual costs should be adequately analysed and reported on to facilitate the cost monitoring. In addition, management should periodically evaluate the results of the IT function's job cost accounting procedures, in light of the organisation's other financial measurement systems.

6.3 User Billing and Chargeback Procedures

CONTROL OBJECTIVE

IT management should define and use billing and chargeback procedures. It should maintain user billing and chargeback procedures that encourage the proper usage of computer resources and assure the fair treatment of user departments and their needs. The rate charged should reflect the associated costs of providing services.

Figure 43—Control Practices for *Identify and Allocate Costs*

DS6.1 Chargeable Items

Why Do It?
The existence of a process and tools for the identification, assessment and formalisation of all chargeable items in line with the control practices will help:
- Improve management understanding and acceptance of IT costs, thereby facilitating more effective budgeting for IT services
- Empower user management with reliable, transparent information about controllable IT costs to facilitate more efficient control and prioritisation of resources
- Enable business management to see the total cost of each business function and, therefore, make better informed decisions

Control Practices
1. There is a clearly defined process of identification and assessment of IT costs at all levels. There is a comprehensive understanding of total costs incurred and the allocation of these costs to business processes.
2. Training is provided to ensure that there is a common understanding of the cost identification approach.
3. There is a clearly defined process in place to facilitate the measurement and costing of IT resources used. The process can guarantee the completeness and accuracy of the measurement and costing as well as the integrity of the subsequent reporting. To the greatest extent possible, the process is—at least in part—based on actual resource usage.
4. A process is in place to allow users to adjust their use of IT resources according to their specific business requirements, and to understand the impact of changes on the associated billing levels.

DS6.2 Costing Procedures

Why Do It?
The existence of an effective IT costing procedure in line with the control practices will help:
- Enable an effective and reliable budgeting process, resulting in the ability to understand and measure variations to costs, and enable costs to be charged back in a timely manner
- Provide reliable information to the organisation about its total IT cost

Control Practices
1. The responsibility for the preparation and maintenance of financial records is identified and the required skills for these tasks are available within the organisation. Internal and external cost management experts are used to the extent needed.
2. A formal process exists for the annual drafting of the IT budget in line with the business budgeting process. The specific budget includes all relevant IT components and expected recovery of costs from business units.
3. An established, auditable process is in place for the accurate and reliable identification, authorisation and accumulation of all costs incurred within the IT department and by third-party service providers. Where possible, the identification of costs is automated, and these automated processes are audited regularly to ensure the accuracy and completeness of the captured data and subsequent reporting.
4. A formal, frequent review and reporting of actual costs are performed. This includes, but is not limited to, tasks such as comparisons to budget, investigation of variations and reforecasting. Specific IT measures may also be included for comparison purposes, such as benchmarking of services against an external market or similar organisations, and assessment of per-unit costing.
5. There are a formal assessment and reporting to management of the IT costing structures.

DS6.3 User Billing and Chargeback Procedures

Why Do It?
Implementing formal user billing and chargeback procedures in line with the control practices will help:
- Improve the opportunity for internal and external benchmarking at a process level
- Promote more effective alignment between business objectives and the cost of IT
- Facilitate the allocation of IT resources to competing IT projects and processes
- Enable business units to fully understand the total IT cost involved for delivering various business processes
- Increase the level of productivity and expand the business view and professionalism of staff within the IT organisation through increased financial accountability

Figure 43—Control Practices for *Identify and Allocate Costs (cont.)*

Control Practices

1. The basis for chargeback and the various components in the calculation (e.g., the direct and indirect costs) have been negotiated and approved with the respective business owners. There is sufficient detail to identify opportunities for cost reduction or instances where unanticipated costs are being incurred. In addition, the benefits of a cost are clearly aligned with the respective aspect of the service level agreement.
2. The process is facilitated through open communication between users and IT management, and concerns regarding specific costing measures are discussed.
3. A process exists for the continual reassessment of the appropriateness of chargeback algorithms after consideration of current actual performance.

Figure 44—Audit Guidelines for *Identify and Allocate Costs*

DS6 IDENTIFY AND ALLOCATE COSTS

CONTROL OBJECTIVES	
1	Chargeable items
2	Costing procedures
3	User billing and chargeback procedures

BOTH HIGH-LEVEL AND DETAILED CONTROL OBJECTIVES ARE AUDITED BY:

Obtaining an understanding by:

► **Interviewing:**

IT administration or cost allocation management
Selected user management charged back and absorbing costs

► **Obtaining:**

Organisationwide polices and procedures relating to planning and budget preparation
IT policies and procedures relating to cost aggregation, chargeback methodology and performance/cost reporting
The IT function's:

- Current and prior year budget
- Tracking reports of IT resource utilisation
- Raw data used in preparing tracking reports
- Cost allocation methodology or algorithm
- Historical chargeback reports

User management's:

- Current and prior year budget for IT costs
- Current year information systems development and maintenance plan
- Budgeted expenses for IT resources, including those charged back or absorbed

Evaluating the controls by:

► **Considering whether:**

IT function has a group responsible for reporting and issuing chargeback bills to users
Procedures are in place that:

- Develop a yearly development and maintenance plan with user identification of priorities for development, maintenance and operational expenses
- Allow for a very high level of user determination of where IT resources are spent
- Generate a yearly IT budget including:
  - Compliance to organisational requirements in budget preparation
  - Consistency with what costs are to be allocated by the user departments

Figure 44—Audit Guidelines for *Identify and Allocate Costs (cont.)*

  - Communication of historical costs, assumptions for new costs— for understanding by users of what costs are included in chargeback
  - User sign-off on all budget costs to be allocated by IT function
  - Frequency of reporting and actual charging of costs to users
- Track allocated costs of all IT resources of, but not limited to:
  - Operational hardware
  - Peripheral equipment
  - Telecommunications usage
  - Applications development and support
  - Administrative overhead
  - External vendor service costs
  - Help desk
  - Facilities and maintenance
  - Direct/indirect costs
  - Fixed and variable expenses
  - Sunk and discretionary costs
- Ensure the regular reporting to users on performance for the various cost categories
- Report to users on external benchmarks regarding cost-effectiveness to allow comparison to industry expectations, or user alternative sourcing for services
- Ensure the timely modification to cost allocations to reflect changing business needs
- Formally approve and accept charges as received
- Identify IT improvement opportunities to reduce chargebacks or get greater value for chargebacks

Reports provide assurance that chargeable items are identifiable, measurable and predictable

Reports capture and highlight changes in the underlying cost components or allocation algorithm

Assessing the compliance by:

► **Testing that:**

A cost allocation methodology exists, is agreed with users for equity, and is generating costs and reports, regarding calculation to confirm

An improvement programme to reduce costs or increase performance of IT resources exists

Allocation and reporting encourage the most proper, effective and consistent use of IT resources, assure fair treatment of user departments and their needs, and charge rates that reflect the associated costs of providing services

Substantiating the risk of control objectives not being met by:

► **Performing:**

Benchmarking of cost accounting and chargeback methodologies against other similar organisations or appropriate international standards/recognised industry best practices

Recalculation of chargeback from raw data, through chargeback allocation algorithm, and into user report streams

Figure 44—Audit Guidelines for *Identify and Allocate Costs (cont.)*

Tests to confirm data in performance reporting is accurate, such as:
- CPU usage
- Peripheral usage
- DASD usage
- Lines of code written
- Lines/pages printed
- Program changes made
- Number of PCs, telephones and data files
- Help desk inquiries
- Number, length of transmissions

Tests to ensure that compilation of raw information resource data into performance reporting is correct

Tests to verify the actual algorithm for compiling and allocating costs into chargeback exists

Tests to confirm the accuracy of chargebacks to specific users is tested frequently

Tests to confirm the chargebacks to users are approved

Consistency checks of chargebacks among different users

Tests to ensure progress on user development plan is based on costs expended

Review of report distribution for usage and cost information

Review of user satisfaction with:
- Reasonableness of chargebacks against budgeted expectations
- Yearly development plan progress vs. charged-back costs
- Reasonableness of chargebacks against alternative sources (i.e., benchmarks)
- Communications of trends that would increase/decrease chargeback
- Resolution of variances from expected chargeback

► **Identifying:**

Opportunities for increased effectiveness and appropriateness of chargeback methodology:
- Including more cost components
- Modifying cost allocation indexes or units of measure
- Modifying cost algorithm itself
- Mechanising or integrating the job accounting function between equipment and application-generating reports

Inconsistencies within the allocation algorithm

Inconsistencies of allocation among different users

Opportunities for systems resource improvements

Improved opportunities for the user to better apply IT resources to accomplish user business requirements

Improved efficiencies in the gathering, accumulation, allocation, reporting and communication process that will translate to improved performance or less cost to users for services provided

Translation of cost trends reflected by variance and analysis into modified charges in subsequent periods and reflection in cost structure

Opportunities to make the IT function a profit centre, rather than a cost centre, by providing services to other internal or external users

If the IT function is a profit centre, that the contribution to profit against plan and budget is being met and opportunities for increased profitability are outlined

Figure 45—Management Guidelines for *Identify and Allocate Costs*

DS6 Deliver and Support
Identify and Allocate Costs

Information Criteria	
	Effectiveness
P	Efficiency
	Confidentiality
	Integrity
	Availability
	Compliance
P	Reliability

(**P**) primary (**S**) secondary

IT Resources
✓ People
✓ Applications
✓ Technology
✓ Facilities
✓ Data

(✓) applicable to

Control over the IT process ***identify and allocate costs*** with the business goal of ensuring a correct awareness of the costs attributable to IT services

ensures delivery of information to the business that addresses the required information criteria and is measured by key goal indicators

is enabled by a cost accounting system that ensures that costs are recorded, calculated and allocated to the required level of detail and to the appropriate service offering

considers critical success factors that leverage specific IT resources and is measured by key performance indicators

Key Goal Indicators

- Continued cost optimisation of information services by the IT function
- Continued cost optimisation of information services by users
- Increased ratio of proven benefits to actual costs of IT services
- Index of efficiency, based on a comparison of internal with external provider costs
- Business management understanding/ acceptance of IT costs and service levels

Critical Success Factors

- End users, business process owners and the IT organisation share a common understanding of costing requirements and cost allocation.
- Direct and indirect costs are identified, captured, reported and analysed in a timely and automated manner.
- Costs are charged back on the basis of utilisation and recorded in chargeback principles that are formally accepted and regularly reassessed.
- Cost reporting is used by all parties to review budget performance, identify cost optimisation opportunities and benchmark performance against reliable sources.
- There is a direct link between the cost of the service and the service level agreements.
- The results of cost allocation and optimisation are used to verify benefit realisation and are fed back into the next budget cycle.

Key Performance Indicators

- Percentage of variance amongst budgets, forecasts and actual costs
- Percentage reduction in information service rates
- Percentage increase in optimisation of user service requests
- Percentage increase in optimisation of IT resources usage
- Number of cost optimisation initiatives

Figure 45—Management Guidelines for *Identify and Allocate Costs (cont.)*

DS6 Maturity Model

Control over the IT process ***identify and allocate costs*** with the business goal of ensuring a correct awareness of the costs attributable to IT services

0 **Nonexistent**—There is a complete lack of any recognisable process for identifying and allocating costs with respect to information services provided. The organisation has not even recognised that there is an issue to be addressed with respect to cost accounting and there is no communication about the issue.

1 **Initial/*Ad Hoc***—There is a general understanding of the overall costs for information services, but there is no breakdown of costs per user, department, groups of users, service functions, projects or deliverables. There is virtually no cost monitoring, with only aggregate cost reporting to management. There is no chargeback process or system in place to bill users for costs incurred in delivering information services.

2 **Repeatable but Intuitive**—There is overall awareness of the need to identify and allocate costs. Cost allocation is based on informal or rudimentary cost assumptions, e.g., hardware costs, and there is virtually no linking to value drivers. Cost allocation processes are repeatable and some of them begin to be monitored. There is no formal training and communication on standard cost identification and allocation procedures. Responsibility is not assigned.

3 **Defined Process**—There is a defined and documented information services cost model. The model is institutionalised and communicated, and informal training is established. An appropriate level of awareness exists of the costs attributable to information services. An automated cost accounting system exists, but is focused on the information services function rather than on business processes.

4 **Managed and Measurable**—Information services cost management responsibilities and accountabilities are defined and fully understood at all levels and are supported by formal training. Direct and indirect costs are identified and reported in a timely and automated manner to management, business process owners and users. Generally, there is cost monitoring and evaluation, and actions are taken when processes are not working effectively or efficiently. Action is taken in many, but not all cases. Cost management processes are continuously being improved and enforce best internal practice. Information services cost reporting is linked to business objectives and service level agreements. There is involvement of all required internal cost management experts.

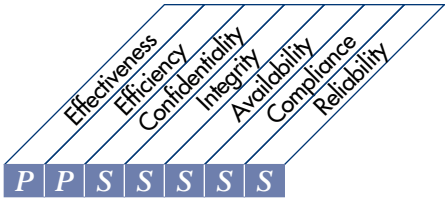
5 **Optimised**—Costs of services provided are identified, captured, summarised and reported to management, business process owners and users. Costs are identified as chargeable items and support a chargeback system that appropriately bills users for services provided, based on utilisation. Cost details support service level agreements. There is strong monitoring and evaluation of costs of services, where variances from budget amounts are identified and discrepancies are detailed and appropriately acted upon. Cost figures obtained are used to verify benefit utilisation and are used in the organisation's budgeting process. Information services cost reporting provides early warning of changing business requirements through intelligent reporting systems. A variable cost model is utilised, derived from volumes processed for each service provided. Cost management has been refined to a level of best practices, based on the result of continuous improvement and maturity modelling with other organisations. External experts are leveraged and benchmarks are used for cost management guidance.

Figure 46—Control Objectives for *Monitor the Process*

HIGH-LEVEL CONTROL OBJECTIVE

M1 Monitor and Evaluate

Monitor the Processes



Control over the IT process of

monitoring the processes

that satisfies the business requirement

to ensure the achievement of the performance objectives set for the IT processes

is enabled by

the definition of relevant performance indicators, the systematic and timely reporting of performance and prompt acting upon deviations

and takes into consideration

- Scorecards with performance drivers and outcome measures
- Customer satisfaction assessments
- Management reporting
- Knowledge base of historical performance
- External benchmarking

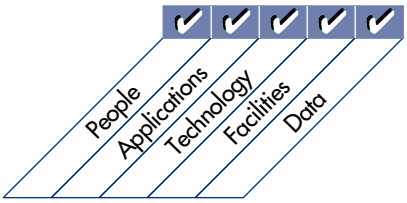


Figure 46—Control Objectives for *Monitor the Process (cont.)*

DETAILED CONTROL OBJECTIVES

1 MONITOR THE PROCESSES

1.1 Collecting Monitoring Data

CONTROL OBJECTIVE

For the IT and internal control processes, management should ensure that relevant performance indicators (e.g., benchmarks) from internal and external sources are defined and data are collected for the creation of management information reports and exception reports regarding these indicators. Controls should also be aimed at validating the propriety and integrity of both organisational and individual performance measures and indicators.

1.2 Assessing Performance

CONTROL OBJECTIVE

Services to be delivered by the IT function should be measured (key performance indicators and/or critical success factors) by management and compared with target levels. Assessments of the IT function should be performed on a continuous basis.

1.3 Assessing Customer Satisfaction

CONTROL OBJECTIVE

At regular intervals, management should measure customer satisfaction regarding the services delivered by the IT function to identify shortfalls in service levels and establish improvement objectives.

1.4 Management Reporting

CONTROL OBJECTIVE

Management reports should be provided for senior management's review of the organisation's progress toward identified goals. Status reports should include the extent to which planned objectives have been achieved, deliverables obtained, performance targets met and risks mitigated. Upon review, appropriate management action should be initiated and controlled.

Figure 47—Control Practices for *Monitor the Processes*

M1.0 Monitoring Approach

Why Do It?
The establishment of an IT performance monitoring framework and approach that is in line with the control practices will:
- Facilitate the achievement of enterprise and IT goals and objectives, quantification of problems, evaluation of alternatives, allocation of resources, progress tracking and learning from mistakes
- Promote efficiency and effectiveness by defining the IT activities, the necessary inputs and the outputs that will result from the process
- Enable more informed IT investment decisions by using comprehensive performance information
- Ensure consistent application of the right number of performance indicators

Control Practices
1. The approach is defined for the implementation and maintenance of an IT performance management system that drives the definition, collection and assessment of performance data. IT processes are focused on and aligned with business strategy and are included in the IT strategy and plan. This ensures that required monitoring activities are compliant with applicable laws and regulations.
2. The IT processes that produce the IT services and their linkage to the business processes are modelled and prioritised. In addition, the model is approved by business management, and then accountability for each process objective is agreed with the process owner.
3. IT process monitoring activities are defined to prevent ineffective information flows and duplication of effort across the Plan and Organise, Acquire and Implement, and Deliver and Support process domains.
4. IT processes are implemented to measure process execution through a diversity of metrics at the individual, organisational, program and process levels. They reflect successful achievement and are useful to direct improvements when goals are not achieved. Measurement results in balanced scorecards are reported and incorporated in the business balanced scorecard.
5. Self-monitoring, analysis and reporting technology (SMART) performance targets are set based on realistic benchmarking, and the reported performance is evaluated regularly. Performance targets reflect business expectations. Individual process performance targets are set in function of the overall business objectives.
6. Formal approval of the measurement framework and performance targets is obtained by senior IT and business management. The measurement framework and performance targets are communicated to and agreed by all process stakeholders.
7. Independent reviews of the performance measurement systems are conducted regularly and the measures are revised or updated in accordance with management feedback or changing business needs. The monitoring approach and framework are revisited on at least an annual basis.

M1.1 Collecting Monitoring Data

Why Do It?
The collection of monitoring data in line with the control practices will:
- Enable effective reporting on organisationwide IT process performance indicators based on relevant data that are appropriate, accurate and timely
- Ensure that systems can efficiently provide the data required to monitor the processes
- Establish a history of organisational performance to monitor trends and changes in performance

Control Practices
1. A policy is designed, exposed for review, approved and implemented that requires data collection aligned with the monitoring approach and commensurate with the level of readiness of, and automation within, the organisation. Accuracy, reliability, timeliness, frequency, measurement technique, data source, storage and security of collected data are considered.
2. Existing data collection and reporting are reviewed regularly, and necessary changes are implemented after obtaining approval.
3. An organisationwide data model encompassing all performance data sources is established. Attributes of this model include data definition, identified source systems (manual or automated), data volumes, frequency of update and external data requirements.
4. Training is provided to ensure that the organisation has adequate skills in measurement, data collection and analysis.
5. Data collection requirements are included as part of the development and acquisition process.
6. Reconciliation and control checks are completed at agreed intervals to assess the integrity of the data collected.
7. A knowledge base of all monitoring data is established and maintained to allow monitoring of trends and changes in performance.

Figure 47—Control Practices for *Monitor the Processes (cont.)*

M1.2 Assessing Performance

Why Do It?
Assessing performance of the services provided by the IT processes along the lines of the control practices will:
- Provide a greater level of accountability and ownership of the performance within the organisation
- Increase the number of process improvement opportunities detected and acted upon
- Reduce the number of outstanding process deficiencies

Control Practices
1. The performance assessment system for information and services to be delivered by the IT processes is defined and agreed with by senior management, taking into account the organisational culture and IT process maturity.
2. Performance indicators are developed from internal and external sources that are verified by management and peers and through self-assessments. Clear accountability is established in performance contracts. Performance indicators are established for financial, operational, customer and organisational learning aspects.
3. Target performance levels are established and the measured performance is compared to the targets at agreed intervals. When targets are not met, the root causes of poor performance are analysed and countermeasures are formulated. When targets are met or exceeded, a formal performance feedback system is in place to recognise and reward exemplary contributions.
4. A comparison to external benchmarking data (industry and key competitors) is formalised, with well-understood criteria.
5. A formal issue-tracking system is implemented to follow all noted performance deviations with a formal close-out of the agreed correction/improvement.

M1.3 Assessing Customer Satisfaction

Why Do It?
Assessing customer satisfaction in line with the control practices will:
- Establish a strong customer bias in the culture of the IT organisation for all IT processes
- Ensure that customer expectations and business needs are identified
- Improve the levels of customer satisfaction and focus by identifying shortfalls in service delivery and implementing improvement opportunities

Control Practices
1. The portfolio of metrics that systematically measure the levels of customer satisfaction is identified. Senior IT and appropriate business management as well as external experts in the development of the customer satisfaction questionnaire are involved.
2. Regular customer feedback and interaction, through surveys and other assessment techniques, are integral parts of the IT performance measurement system.
3. Performance levels are documented, communicated and formally agreed by customers, as required by service level agreements.
4. Key performance measures of customer satisfaction are monitored and reported to all stakeholders, particularly the customers. These measurements are acted upon, whilst the confidentiality and integrity of survey results are maintained.

M1.4 Management Reporting

Why Do It?
Management reporting in line with the control practices will:
- Ensure that performance information can be effectively and efficiently used for strategic, managerial and day-to-day operations.
- Enhance the decision-making processes in responding to business needs and concerns, and focus on process improvement opportunities
- Increase satisfaction of management and its governance with performance reporting

Control Practices
1. A management process is established for regular, accurate and timely reporting on, and subsequent analysis of, the agreed criteria at the appropriate level of aggregation (i.e., enforce reporting and promote the analysis and discussion of trends, issues and potential implications).
2. Concise and easy-to-understand IT performance reports are designed and tailored to various management needs and audiences, including governance. More efficient and effective methods to present the performance information to management are developed to facilitate better decision-making. The reports are structured so that process interdependencies and their cause-effect implications are communicated in an understandable manner.
3. The performance measurement results are populated into the IT balanced scorecards, traffic light reports or other monitoring tools. Then, the delivery is evaluated against the IT strategy.

Figure 48—Audit Guidelines for *Monitor the Processes*

M1 MONITOR THE PROCESSES

CONTROL OBJECTIVES	
1	Collecting monitoring data
2	Assessing performance
3	Assessing customer satisfaction
4	Management reporting

BOTH HIGH-LEVEL AND DETAILED CONTROL OBJECTIVES ARE AUDITED BY:

Obtaining an understanding by:

- **Interviewing:**

  Chief executive officer
  Chief information officer
  Senior internal audit officer
  IT senior and quality control management
  External audit senior manager
  Selected users of IT resources
  Audit committee members, if applicable

- **Obtaining**

  Organisationwide policies and procedures relating to planning, managing, monitoring and reporting on performance
  IT policies and procedures relating to monitoring and reporting on performance, establishing performance improvement initiatives and frequency of review
  Reports of IT activities including, but not limited to, internal reports, internal audit reports, external audit reports, user reports, user satisfaction surveys, system development plans and status reports, audit committee minutes and any other assessments of the organisation's use of IT resources
  Information services function planning documents with deliverables for each resource group and actual performance against those plans

Evaluating the controls by:

- **Considering whether:**

  Data identified for monitoring IT resources are appropriate
  Key performance indicators and/or critical success factors are used to measure IT performance against target levels
  Internal reporting of IT resource utilisation (people, facilities, applications, technology and data) is adequate
  Managerial review of IT resource performance reporting exists

Figure 48—Audit Guidelines for *Monitor the Processes (cont.)*

Monitoring controls exist to provide reliable and useful feedback in a timely manner
Response of organisation to quality control, internal audit and external audit improvement recommendations is appropriate
Target performance improvement initiatives and results exist
Organisational performance against stated goals of all groups within the organisation is occurring
User satisfaction analysis exists
Reliability and usability of performance reporting for nonusers such as external auditor, audit committee and senior management of the whole organisation are sufficient
Timeliness of reporting allows for rapid response to identified performance shortcomings or exceptions
Reporting against policies and procedures established for the performance of activities (i.e., performance reporting) is sufficient

Assessing the compliance by:

► **Testing that:**

Data performance monitoring reports exist
Managerial review of performance monitoring reports and corrective action initiatives is occurring
Employees are aware of and understand policies and procedures relating to performance monitoring
Quality and content of internal reporting relate to:
- Collection of performance monitoring data
- Analysis of performance monitoring data
- Analysis of resource performance data
- Management actions on performance issues
- Analysis of user satisfaction surveys

Senior management is satisfied with reporting on performance monitoring

Substantiating the risk of control objectives not being met by:

► **Performing:**

Benchmarking of performance monitoring against similar organisations or appropriate international standards/recognised industry best practices
Review of relevancy of data within processes being monitored
Actual-to-planned performance review in all IT areas
Actual-to-anticipated user satisfaction review of all IT areas
Analysis of extent of accomplishment of performance goals improvement initiatives
Analysis of level of implementation of managerial recommendations

► **Identifying:**

Competence, authority and independence of monitoring staff within the information systems organisation

Figure 49—Management Guidelines for *Monitor the Processes*

M1 Monitor and Evaluate
Monitor the Processes

Control over the IT process ***monitor the processes*** with the business goal of ensuring the achievement of the performance objectives set for the IT processes

ensures delivery of information to the business that addresses the required information criteria and is measured by key goal indicators

is enabled by the definition of relevant performance indicators, the systematic and timely reporting of performance and prompt acting upon deviations

considers critical success factors that leverage specific IT resources and is measured by key performance indicators

Information Criteria
P Effectiveness
P Efficiency
S Confidentiality
S Integrity
S Availability
S Compliance
S Reliability

(**P**) primary (**S**) secondary

IT Resources
✓ People
✓ Applications
✓ Technology
✓ Facilities
✓ Data

(✓) applicable to

Key Goal Indicators

- Consistent application of the right, limited number of performance indicators
- Increased number of process improvement opportunities detected and acted upon
- Satisfaction of management and the governance entity with performance reporting
- Reduced number of outstanding process deficiencies

Key Performance Indicators

- Time lag between the process deficiency occurrence and reporting
- Time lag between the reporting of a deficiency and action initiated
- Ratio between process deficiencies reported and deficiencies subsequently accepted as requiring management attention follow-up (noise index)
- Number of processes monitored
- Number of cause and effect relations identified and incorporated in monitoring
- Number of external benchmarks of process effectiveness
- Time lag between business changes and any associated changes to performance indicators
- Number of changes to the set of performance indicators without the business goals changing

Critical Success Factors

- Useful, accurate and timely management reports are available.
- Processes have defined and understood key goal indicators and key performance indicators.
- Measurements of IT performance include financial, operational, customer and organisational learning criteria that ensure alignment with organisationwide goals and can be integrated with tools such as the IT balanced business scorecard.
- There are clearly understood and communicated process objectives.
- A framework is established for defining and implementing IT governance reporting requirements.
- A knowledge base of historical performance is established.

Figure 49—Management Guidelines for *Monitor the Processes (cont.)*

M1 Maturity Model

Control over the IT process ***monitor the processes*** with the business goal of ensuring the achievement of the performance objectives set for the IT processes

0 **Nonexistent**—The organisation has no monitoring process implemented. IT does not independently perform monitoring of projects or processes. Useful, timely and accurate reports are not available. The need for clearly understood process objectives is not recognised.

1 **Initial/*Ad Hoc***—Management recognises a need to collect and assess information about monitoring processes. Standard collection and assessment processes have not been identified. Monitoring is implemented and metrics are chosen on a case-by-case basis, according to the needs of specific IT projects and processes. Monitoring is generally implemented reactively to an incident that has caused some loss or embarrassment to the organisation. Monitoring is implemented by the information services function for the benefit of other departments, but is not implemented over IT processes. Process definition and monitoring measures follow traditional financial, operations and internal control approaches, without specifically addressing the needs of the information services function.

2 **Repeatable but Intuitive**—Basic measurements to be monitored have been identified. Collection and assessment methods and techniques have been defined, but the processes have not been adopted across the entire organisation. Planning and management functions are created for assessing monitoring processes, but decisions are made based on the expertise of key individuals. Limited tools are chosen and implemented for gathering information, but may not be used to their full capacity due to a lack of expertise in their functionality. The information services function is managed as a cost centre, without assessing its contribution to the revenue-generating entities of the organisation.

3 **Defined Process**—Management has communicated and institutionalised standard monitoring processes. Educational and training programmes for monitoring have been implemented. A formalised knowledge base of historical performance information has been developed. Assessment is still performed at the individual IT process and project level and is not integrated among all processes. Tools for monitoring internal IT processes and service levels are being implemented. Measurements of the contribution of the information services function to the performance of the organisation have been defined, using traditional financial and operational criteria. IT-specific performance measurements are defined and implemented, but the nonfinancial and strategic measurements are still informal. Measures of customer satisfaction and service levels provided to the operating entities of the organisation are being implemented.

4 **Managed and Measurable**—Management has defined the tolerances under which processes must operate. Baselining of monitoring results is being standardised and normalised. There is integration of metrics across all IT projects and processes. The information services function management reporting systems are formalised and fully automated. Automated tools are integrated and leveraged organisationwide to collect and monitor operational information on applications, systems and processes. A framework has been defined for identifying strategically oriented KGIs, KPIs and CSFs to measure performance. Criteria for evaluating organisational development based on maturity models have been defined. Measurements of the information services function performance include financial, operational, customer and organisational learning criteria that ensure alignment with organisationwide goals.

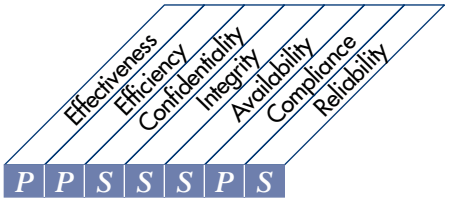
5 **Optimised**—A continuous quality improvement process is developed for updating organisationwide monitoring standards and policies and incorporating industry best practices. All monitoring processes are optimised and support organisationwide objectives. KGIs, KPIs and CSFs are routinely used to measure performance and are integrated into strategic assessment frameworks such as the IT balanced scorecard. Process monitoring and ongoing redesign are consistent with plans developed based on process maturity models and with organisationwide business process improvement plans. Benchmarking against industry and key competitors has become formalised, with well-understood comparison criteria.

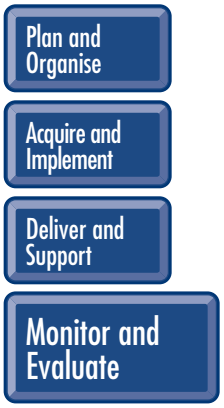
Figure 50—Control Objectives for *Assess Internal Control Adequacy*

HIGH-LEVEL CONTROL OBJECTIVE

M2 Monitor and Evaluate

Assess Internal Control Adequacy





Control over the IT process of

assessing internal control adequacy

that satisfies the business requirement

to ensure the achievement of the internal control objectives set for the IT processes

is enabled by

the commitment to monitoring internal controls, assessing their effectiveness, and reporting on them on a regular basis

and takes into consideration

- Responsibilities for internal control
- Ongoing internal control monitoring
- Benchmarks
- Error and exception reporting
- Self-assessments
- Management reporting
- Compliance with legal and regulatory requirements

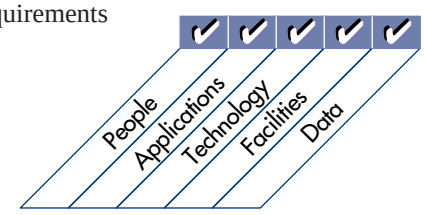


Figure 50—Control Objectives for *Assess Internal Control Adequacy (cont.)*

DETAILED CONTROL OBJECTIVES

2 ASSESS INTERNAL CONTROL ADEQUACY

2.1 Internal Control Monitoring

CONTROL OBJECTIVE

Management should monitor the effectiveness of internal controls in the normal course of operations through management and supervisory activities, comparisons, reconciliations and other routine actions. Deviations should evoke analysis and corrective action. In addition, deviations should be communicated to the individual responsible for the function and at least one level of management above that individual. Serious deviations should be reported to senior management.

2.2 Timely Operation of Internal Controls

CONTROL OBJECTIVE

Reliance on internal controls requires that controls operate promptly to highlight errors and inconsistencies and that these be corrected before they impact production and delivery. Information regarding errors, inconsistencies and exceptions should be kept and systematically reported to management.

2.3 Internal Control Level Reporting

CONTROL OBJECTIVE

Management should report information on internal control levels and exceptions to the affected parties to ensure the continued effectiveness of the internal control system. Actions should be taken to identify what information is needed at a particular level of decision making.

2.4 Operational Security and Internal Control Assurance

CONTROL OBJECTIVE

Operational security and internal control assurance should be established and periodically repeated, with self-assessment or independent audit, to examine whether or not the security and internal controls are operating according to the stated or implied security and internal control requirements. Ongoing monitoring activities by management should look for vulnerabilities and security problems.

Figure 51—Control Practices for *Assess Internal Control Adequacy*

M2.0 Internal Control Framework and Approach

Why Do It?
The establishment of an IT control framework and approach that is in line with the control practices will:
- Facilitate the provision of (third-party) assurance under SSAE 10 or SAS70
- Facilitate the detection of control gaps or overly controlled areas
- Enable the design, implementation and operation of effective monitoring of internal controls

Control Practices
1. Management demonstrates a positive attitude toward internal control, including a clear commitment to act on internal control deficiencies.
2. Organisationwide and information function-specific policies and procedures relating to planning, managing, monitoring and reporting upon internal controls are in place.
3. Building on a formally defined IT control process framework and the results of an organisationwide formal risk analysis, the main areas requiring control (e.g., governance, confidentiality, integrity and availability) are determined. These areas are linked to service commitments as expressed in formal contracts with customers or marketing documentation.
4. For each of the control areas, the high-level control objectives are outlined.
5. For each of the high-level control objectives, the key controls are determined. The accountability, related documentation and supporting evidence for each of the key controls are documented.
6. The organisation's control policy and related processes provide for adequate training on internal control and the organisation's control policy, as well as responsibilities.
7. A formal IT control function, with specialised and certified professionals, is established.
8. The competence and authority of the internal control compliance function are regularly and independently assessed and maintained or improved as needed.
9. Responsibilities for internal control and compliance are formally assigned, published and included in training to ensure that they are clearly understood.

M2.1 Internal Control Monitoring

Why Do It?
Monitoring the effectiveness of internal controls in line with the control practices will:
- Ensure the presence and functioning of internal control components over time
- Ensure that required control improvements are initiated and deployed
- Help achieve the organisation's objectives
- Ensure that internal control withstands the scrutiny of regulators (e.g., US Securities and Exchange Commission)
- Ensure that assurance is available for IT decisions when needed
- Help reduce overhead of obtaining assurance and certifications

Control Practices
1. A policy is adopted that requires ongoing monitoring activities (e.g., management and supervisory activities, variance analysis, stress testing, comparisons, reconciliations or other routine actions) and separate evaluations of the internal control system. The policy requires that ongoing monitoring be built into the normal, recurring operating activities of an organisation.
2. Automated or manual processes are implemented for the timely, complete and accurate execution of control activities and reporting. At the highest level, the reporting results in a dashboard or balanced scorecard, reflecting the state of internal control within the organisation. Data are analysed over time to detect underperforming areas requiring corrective action (reinforcement of internal controls).
3. Accountability and responsibility are assigned for the monitoring of internal controls and reporting of issues to the appropriate level of management, ensuring that required corrective actions will be deployed. Depending on the potential impact of internal control issues, they may have to be reported to multiple levels of management and possibly to the board of directors or oversight groups.
4. Processes or procedures are established to ensure that control exceptions are promptly reported, followed up and analysed, and corrective actions are chosen and implemented. Use of existing change and problem management procedures is recommended.

Figure 51—Control Practices for *Assess Internal Control Adequacy (cont.)*

5. Processes and procedures are in place to ensure that internal control monitoring data are accurate, complete and timely.
6. A continuous improvement process is in place to ensure that internal control monitoring is improved if IT decisions fail, or reversed after positive assurance is obtained.

M2.2 Timely Operation of Internal Controls

Why Do It?
The timely operation of internal controls in line with the control practices will:
- Ensure that control violations, errors and inconsistencies are promptly identified, thus minimising the impact on the organisation's operations or reputation
- Ensure that supporting evidence and context are safeguarded for analysis and review, allowing for the timely resolution of causes of control failure to avoid reoccurrence

Control Practices
1. The organisation's internal control policy sets the expectation that controls are designed to be effective, taken seriously and performed on a timely basis.
2. The organisation's internal control policy requires the safeguarding of evidence of control exceptions for review and analysis, and exceptions are reported routinely to the required level of management.
3. Procedures to ensure that controls are executed when needed are developed and implemented, and the failure to do so is reported, minimising the time lag between internal control deficiency occurrences and reporting.
4. Procedures are developed to ensure the timely resolution of any control failures, including safeguarding supporting evidence, root cause analysis and prompt implementation of corrective measures.

M2.3 Internal Control Level Reporting

Why Do It?
Internal control level reporting in line with the control practices will:
- Ensure that the right level of management is informed of control deficiencies and involved in the resolution of any such issues

Control Practices
1. Thresholds are established for levels of control exceptions and control breakdowns, considering the risks involved for the organisation.
2. The appropriate levels of management needed when surpassing set control thresholds are determined and accountability for reporting and taking action is assigned accordingly.

M2.4 Operational Security and Internal Control Assurance

Why Do It?
Establishing operational security and internal control assurance in line with the control practices will:
- Ensure the presence and continuous functioning of internal controls over time

Control Practices
1. The need for and frequency of independent evaluations of the operational security and internal control environment are determined, taking into account management's assessment of the degree and effectiveness of ongoing monitoring.
2. Processes for performance of separate evaluations are established, ensuring objectivity and rigour independent of the evaluation technique used (e.g., control self-assessment where risk management is the responsibility of everyone within the organisation, or general/application control reviews by internal or external auditors).
3. Independent reviews of the internal control framework by experienced and qualified experts are established. The minimum frequency for such reviews is determined. Benchmarking against industry standards and best practices is part of such reviews.
4. Processes are established for maintaining capability and maturity in line with best practice via capability assessments, benchmarking and continuous improvement strategies, such as strategic partnering.

Figure 52—Audit Guidelines for *Assess Internal Control Adequacy*

M2 ASSESS INTERNAL CONTROL ADEQUACY

CONTROL OBJECTIVES	
1	Internal control monitoring
2	Timely operation of internal controls
3	Internal control level reporting
4	Operational security and internal control assurance

BOTH HIGH-LEVEL AND DETAILED CONTROL OBJECTIVES ARE AUDITED BY:

Obtaining an understanding by:

- **Interviewing:**

  Chief executive officer
  Chief information officer
  Senior internal audit officer
  IT senior and quality control management
  External audit senior manager
  Selected users of IT resources
  Audit committee members, if applicable

- **Obtaining**

  Organisationwide policies and procedures relating to planning, managing, monitoring and reporting upon internal controls
  IT policies and procedures relating to monitoring and reporting on internal controls and frequency of review
  Reports of IT activities including, but not limited to, internal reports, internal audit reports, external audit reports, user reports, system development plans and status reports, audit committee minutes and any other assessments of IT internal controls
  Specific IT policies and procedures relating to operational security and internal control assurance

Evaluating the controls by:

- **Considering whether:**

  Data identified for monitoring IT internal controls are appropriate
  Internal reporting of IT internal control data is adequate
  Managerial review of IT internal controls exists
  Monitoring controls exist to provide reliable and useful feedback in a timely manner
  Response of organisation to quality control, internal audit and external audit improvement recommendations is appropriate
  Target internal control improvement initiatives and results exist

Figure 52—Audit Guidelines for *Assess Internal Control Adequacy (cont.)*

Organisational performance against stated goals of internal controls is occurring
Information regarding internal control errors, inconsistencies and exceptions is systematically kept and reported to management
Reliability and usability of internal control reporting for nonusers such as external auditor, audit committee and senior management of the whole organisation are sufficient
Timeliness of reporting allows for rapid response to identified internal control shortcomings or exceptions
Internal control reporting against policies and procedures established for the performance of activities (i.e., internal control reporting) is sufficient

Assessing the compliance by:

► **Testing that:**

Internal control monitoring reports exist
Managerial review of internal control reports and corrective action initiatives is occurring
Employees are aware of and understand policies and procedures relating to internal control monitoring
Quality and content of internal reporting relate to:
- Collection of internal control monitoring data
- Internal control compliance performance
- Management actions on internal control issues
- Operational security and internal control assurance

Senior management is satisfied with reporting on security and internal control monitoring

Substantiating the risk of control objectives not being met by:

► **Performing:**

Benchmarking of internal control assessment against similar organisations or appropriate international standards/recognised industry best practices
Review of relevancy of data within processes being monitored and in internal controls reporting
Internal controls review framework of the overall organisation and IT specifically to ensure sufficiency of coverage and various levels of details for process owners
Actual to planned internal control review in all IT areas
Analysis of extent of accomplishment of internal control goals improvement initiatives
Review of audit committee's satisfaction with reporting on internal controls
Analysis of level of implementation of managerial recommendations

► **Identifying:**

Additional areas for possible internal control reporting consistent with IT audit, management, external auditor and regulatory concerns
Competence, authority and independence of internal control review staff within the information systems organisation

Figure 53—Management Guidelines for *Assess Internal Control Adequacy*

M2 Monitor and Evaluate
Assess Internal Control Adequacy

Control over the IT process ***assess internal control adequacy*** with the business goal of ensuring the achievement of the internal control objectives set for the IT processes

ensures delivery of information to the business that addresses the required information criteria and is measured by key goal indicators

is enabled by the commitment to monitoring internal controls, assessing their effectiveness, and reporting on them on a regular basis

considers critical success factors that leverage specific IT resources and is measured by key performance indicators

Information Criteria
P Effectiveness
P Efficiency
S Confidentiality
S Integrity
S Availability
P Compliance
S Reliability

(**P**) primary (**S**) secondary

IT Resources
✓ People
✓ Applications
✓ Technology
✓ Facilities
✓ Data

(✓) applicable to

Critical Success Factors

- Management clearly defines what components of the processes need to be controlled.
- Internal control, compliance and internal audit responsibilities are clearly understood.
- Competence and authority of the internal control compliance function exist, addressing delegation as appropriate.
- A properly defined IT control process framework is in place.
- A clear process is used for timely reporting of internal control deficiencies.
- Internal control monitoring data are accurate, complete and timely.
- There is management commitment to act on internal control deficiencies.
- There is alignment with risk assessment and security processes.
- A process is in place to support knowledge sharing on internal control incidents and solutions.

Key Goal Indicators

- Index of senior management satisfaction and comfort with reporting on internal control monitoring
- Decreased probability of internal control incidents
- Positive external qualification and certification reports
- Number of control improvement initiatives
- Absence of regulatory or legal noncompliance events
- Decreased number of security incidents and quality defects

Key Performance Indicators

- Number and coverage of control self-assessments
- Timeliness between internal control deficiency occurrence and reporting
- Number, frequency and coverage of internal compliance reports
- Number of timely actions on internal control issues
- Number of control improvements stemming from root cause analysis

Figure 53—Management Guidelines for *Assess Internal Control Adequacy (cont.)*

M2 Maturity Model

Control over the IT process ***assess internal control adequacy*** with the business goal of ensuring the achievement of the internal control objectives set for the IT processes

0 **Nonexistent**—The organisation lacks procedures to monitor the effectiveness of internal controls. Management internal control reporting methods are absent. There is a general unawareness of IT operational security and internal control assurance. Management and employees have an overall lack of awareness of internal controls.

1 **Initial/*Ad Hoc***—The organisation has a lack of management commitment for regular operational security and internal control assurance. Individual expertise in assessing internal control adequacy is applied on an *ad hoc* basis. IT management has not formally assigned responsibility for monitoring effectiveness of internal controls. IT internal control assessments are conducted as part of traditional financial audits, with methodologies and skill sets that do not reflect the needs of the information services function.

2 **Repeatable but Intuitive**—The organisation uses informal control reports to initiate corrective action initiatives. Planning and management processes are defined, but assessment is dependent on the skill sets of key individuals. The organisation has an increased awareness of internal control monitoring. Management has begun to establish basic metrics. Information services management performs monitoring over the effectiveness of critical internal controls on a regular basis. Controls over security are monitored and results are reviewed regularly. Methodologies and tools specific to the IT environment are starting to be used, but not consistently. Skilled IT staff is routinely participating in internal control assessments. Risk factors specific to the IT environment are being defined.

3 **Defined Process**—Management supports and has institutionalised internal control monitoring. Policies and procedures have been developed for assessing and reporting on internal control monitoring activities. A metrics knowledge base for historical information on internal control monitoring is being established. An education and training programme for internal control monitoring has been implemented. Peer reviews for internal control monitoring have been established. Self-assessments and internal controls assurance reviews are established over operational security and internal control assurance and involve information services function management working with business managers. Tools are being utilised but are not necessarily integrated into all processes. IT process risk assessment policies are being used within control frameworks developed specifically for the IT organisation. The information system services function is developing its own technically oriented IT internal control capabilities.

4 **Managed and Measurable**—Management has established benchmarking and quantitative goals for internal control review processes. The organisation has established tolerance levels for the internal control monitoring process. Integrated and increasingly automated tools are incorporated into internal control review processes, with an increased use of quantitative analysis and control. Process-specific risks and mitigation policies are defined for the entire information services function. A formal IT internal control function is established, with specialised and certified professionals utilising a formal control framework endorsed by senior management. Benchmarking against industry standards and development of best practices are being formalised.

5 **Optimised**—Management has established an organisationwide continuous improvement programme that takes into account lessons learned and industry best practices for internal control monitoring. The organisation uses state-of-the-art tools that are integrated and updated, where appropriate. Knowledge sharing is formalised and formal training programmes, specific to the information services function, are implemented. IT control frameworks address not only IT technical issues, but are integrated with organisationwide frameworks and methodologies to ensure consistency with organisation goals.