CONTROL OBJECTIVE RELATIONSHIPS DOMAINS, PROCESSES AND CONTROL OBJECTIVES

PLANNING & ORGANISATION

1.0 Define a Strategic IT Plan
- 1.1 IT as Part of the Organisation's Long- and Short-Range Plan
- 1.2 IT Long-Range Plan
- 1.3 IT Long-Range Planning—Approach and Structure
- 1.4 IT Long-Range Plan Changes
- 1.5 Short-Range Planning for the IT Function
- 1.6 Communication of IT Plans
- 1.7 Monitoring and Evaluating of IT Plans
- 1.8 Assessment of Existing Systems

2.0 Define the Information Architecture
- 2.1 Information Architecture Model
- 2.2 Corporate Data Dictionary and Data Syntax Rules
- 2.3 Data Classification Scheme
- 2.4 Security Levels

3.0 Determine Technological Direction
- 3.1 Technological Infrastructure Planning
- 3.2 Monitor Future Trends and Regulations
- 3.3 Technological Infrastructure Contingency
- 3.4 Hardware and Software Acquisition Plans
- 3.5 Technology Standards

4.0 Define the IT Organisation and Relationships
- 4.1 IT Planning or Steering Committee
- 4.2 Organisational Placement of the IT Function
- 4.3 Review of Organisational Achievements
- 4.4 Roles and Responsibilities
- 4.5 Responsibility for Quality Assurance
- 4.6 Responsibility for Logical and Physical Security
- 4.7 Ownership and Custodianship
- 4.8 Data and System Ownership
- 4.9 Supervision
- 4.10 Segregation of Duties
- 4.11 IT Staffing
- 4.12 Job or Position Descriptions for IT Staff
- 4.13 Key IT Personnel
- 4.14 Contracted Staff Policies and Procedures
- 4.15 Relationships

5.0 Manage the IT Investment
- 5.1 Annual IT Operating Budget
- 5.2 Cost and Benefit Monitoring
- 5.3 Cost and Benefit Justification

6.0 Communicate Management Aims and Direction
- 6.1 Positive Information Control Environment
- 6.2 Management's Responsibility for Policies
- 6.3 Communication of Organisation Policies
- 6.4 Policy Implementation Resources
- 6.5 Maintenance of Policies
- 6.6 Compliance with Policies, Procedures and Standards
- 6.7 Quality Commitment
- 6.8 Security and Internal Control Framework Policy
- 6.9 Intellectual Property Rights
- 6.10 Issue-Specific Policies
- 6.11 Communication of IT Security Awareness

7.0 Manage Human Resources
- 7.1 Personnel Recruitment and Promotion
- 7.2 Personnel Qualifications
- 7.3 Roles and Responsibilities
- 7.4 Personnel Training
- 7.5 Cross-Training or Staff Back-up
- 7.6 Personnel Clearance Procedures
- 7.7 Employee Job Performance Evaluation
- 7.8 Job Change and Termination

8.0 Ensure Compliance with External Requirements
- 8.1 External Requirements Review
- 8.2 Practices and Procedures for Complying with External Requirements
- 8.3 Safety and Ergonomic Compliance
- 8.4 Privacy, Intellectual Property and Data Flow
- 8.5 Electronic Commerce
- 8.6 Compliance with Insurance Contracts

DOMAINS, PROCESSES AND CONTROL OBJECTIVES

PLANNING & ORGANISATION *continued*

9.0 Assess Risks
- 9.1 Business Risk Assessment
- 9.2 Risk Assessment Approach
- 9.3 Risk Identification
- 9.4 Risk Measurement
- 9.5 Risk Action Plan
- 9.6 Risk Acceptance
- 9.7 Safeguard Selection
- 9.8 Risk Assessment Commitment

10.0 Manage Projects
- 10.1 Project Management Framework
- 10.2 User Department Participation in Project Initiation
- 10.3 Project Team Membership and Responsibilities
- 10.4 Project Definition
- 10.5 Project Approval
- 10.6 Project Phase Approval
- 10.7 Project Master Plan
- 10.8 System Quality Assurance Plan
- 10.9 Planning of Assurance Methods
- 10.10 Formal Project Risk Management
- 10.11 Test Plan
- 10.12 Training Plan
- 10.13 Post-Implementation Review Plan

11.0 Manage Quality
- 11.1 General Quality Plan
- 11.2 Quality Assurance Approach
- 11.3 Quality Assurance Planning
- 11.4 Quality Assurance Review of Adherence to IT Standards and Procedures
- 11.5 System Development Life Cycle Methodology
- 11.6 System Development Life Cycle Methodology for Major Changes to Existing Technology
- 11.7 Updating of the System Development Life Cycle Methodology
- 11.8 Coordination and Communication
- 11.9 Acquisition and Maintenance Framework for the Technology Infrastructure
- 11.10 Third-Party Implementor Relationships
- 11.11 Programme Documentation Standards
- 11.12 Programme Testing Standards
- 11.13 System Testing Standards
- 11.14 Parallel/Pilot Testing
- 11.15 System Testing Documentation
- 11.16 Quality Assurance Evaluation of Adherence to Development Standards
- 11.17 Quality Assurance Review of the Achievement of IT Objectives
- 11.18 Quality Metrics
- 11.19 Reports of Quality Assurance Reviews

ACQUISITION & IMPLEMENTATION

1.0 Identify Automated Solutions
- 1.1 Definition of Information Requirements
- 1.2 Formulation of Alternative Courses of Action
- 1.3 Formulation of Acquisition Strategy
- 1.4 Third-Party Service Requirements
- 1.5 Technological Feasibility Study
- 1.6 Economic Feasibility Study
- 1.7 Information Architecture
- 1.8 Risk Analysis Report
- 1.9 Cost-Effective Security Controls
- 1.10 Audit Trails Design
- 1.11 Ergonomics
- 1.12 Selection of System Software
- 1.13 Procurement Control
- 1.14 Software Product Acquisition
- 1.15 Third-Party Software Maintenance
- 1.16 Contract Application Programming
- 1.17 Acceptance of Facilities
- 1.18 Acceptance of Technology

2.0 Acquire and Maintain Application Software
- 2.1 Design Methods
- 2.2 Major Changes to Existing Systems
- 2.3 Design Approval
- 2.4 File Requirements Definition and Documentation
- 2.5 Programme Specifications
- 2.6 Source Data Collection Design

DOMAINS, PROCESSES AND CONTROL OBJECTIVES

- 2.7 Input Requirements Definition and Documentation
- 2.8 Definition of Interfaces
- 2.9 User-Machine Interface
- 2.10 Processing Requirements Definition and Documentation
- 2.11 Output Requirements Definition and Documentation
- 2.12 Controllability
- 2.13 Availability as a Key Design Factor
- 2.14 IT Integrity Provisions in Application Programme Software
- 2.15 Application Software Testing
- 2.16 User Reference and Support Materials
- 2.17 Reassessment of System Design

3.0 Acquire and Maintain Technology Infrastructure

- 3.1 Assessment of New Hardware and Software
- 3.2 Preventative Maintenance for Hardware
- 3.3 System Software Security
- 3.4 System Software Installation
- 3.5 System Software Maintenance
- 3.6 System Software Change Controls
- 3.7 Use and Monitoring of System Utilities

4.0 Develop and Maintain Procedures

- 4.1 Operational Requirements and Service Levels
- 4.2 User Procedures Manual
- 4.3 Operations Manual
- 4.4 Training Materials

5.0 Install and Accredit Systems

- 5.1 Training
- 5.2 Application Software Performance Sizing
- 5.3 Implementation Plan
- 5.4 System Conversion
- 5.5 Data Conversion
- 5.6 Testing Strategies and Plans
- 5.7 Testing of Changes
- 5.8 Parallel/Pilot Testing Criteria and Performance
- 5.9 Final Acceptance Test
- 5.10 Security Testing and Accreditation
- 5.11 Operational Test
- 5.12 Promotion to Production
- 5.13 Evaluation of Meeting User Requirements
- 5.14 Management's Post-Implementation Review

6.0 Manage Changes

- 6.1 Change Request Initiation and Control
- 6.2 Impact Assessment
- 6.3 Control of Changes
- 6.4 Emergency Changes
- 6.5 Documentation and Procedures
- 6.6 Authorised Maintenance
- 6.7 Software Release Policy
- 6.8 Distribution of Software

DELIVERY & SUPPORT

1.0 Define and Manage Service Levels

- 1.1 Service Level Agreement Framework
- 1.2 Aspects of Service Level Agreements
- 1.3 Performance Procedures
- 1.4 Monitoring and Reporting
- 1.5 Review of Service Level Agreements and Contracts
- 1.6 Chargeable Items
- 1.7 Service Improvement Programme

2.0 Manage Third-Party Services

- 2.1 Supplier Interfaces
- 2.2 Owner Relationships
- 2.3 Third-Party Contracts
- 2.4 Third-Party Qualifications
- 2.5 Outsourcing Contracts
- 2.6 Continuity of Services
- 2.7 Security Relationships
- 2.8 Monitoring

3.0 Manage Performance and Capacity

- 3.1 Availability and Performance Requirements
- 3.2 Availability Plan
- 3.3 Monitoring and Reporting
- 3.4 Modeling Tools
- 3.5 Proactive Performance Management
- 3.6 Workload Forecasting
- 3.7 Capacity Management of Resources

DOMAINS, PROCESSES AND CONTROL OBJECTIVES

DELIVERY & SUPPORT *continued*

- 3.8 Resources Availability
- 3.9 Resources Schedule

4.0 Ensure Continuous Service

- 4.1 IT Continuity Framework
- 4.2 IT Continuity Plan Strategy and Philosophy
- 4.3 IT Continuity Plan Contents
- 4.4 Minimising IT Continuity Requirements
- 4.5 Maintaining the IT Continuity Plan
- 4.6 Testing the IT Continuity Plan
- 4.7 IT Continuity Plan Training
- 4.8 IT Continuity Plan Distribution
- 4.9 User Department Alternative Processing Back-up Procedures
- 4.10 Critical IT Resources
- 4.11 Back-up Site and Hardware
- 4.12 Off-site Back-up Storage
- 4.13 Wrap-up Procedures

5.0 Ensure Systems Security

- 5.1 Manage Security Measures
- 5.2 Identification, Authentication and Access
- 5.3 Security of Online Access to Data
- 5.4 User Account Management
- 5.5 Management Review of User Accounts
- 5.6 User Control of User Accounts
- 5.7 Security Surveillance
- 5.8 Data Classification
- 5.9 Central Identification and Access Rights Management
- 5.10 Violation and Security Activity Reports
- 5.11 Incident Handling
- 5.12 Reaccreditation
- 5.13 Counterparty Trust
- 5.14 Transaction Authorisation
- 5.15 Non-Repudiation
- 5.16 Trusted Path
- 5.17 Protection of Security Functions
- 5.18 Cryptographic Key Management
- 5.19 Malicious Software Prevention, Detection and Correction
- 5.20 Firewall Architectures and Connections with Public Networks
- 5.21 Protection of Electronic Value

6.0 Identify and Allocate Costs

- 6.1 Chargeable Items
- 6.2 Costing Procedures
- 6.3 User Billing and Chargeback Procedures

7.0 Educate and Train Users

- 7.1 Identification of Training Needs
- 7.2 Training Organisation
- 7.3 Security Principles and Awareness Training

8.0 Assist and Advise Customers

- 8.1 Help Desk
- 8.2 Registration of Customer Queries
- 8.3 Customer Query Escalation
- 8.4 Monitoring of Clearance
- 8.5 Trend Analysis and Reporting

9.0 Manage the Configuration

- 9.1 Configuration Recording
- 9.2 Configuration Baseline
- 9.3 Status Accounting
- 9.4 Configuration Control
- 9.5 Unauthorised Software
- 9.6 Software Storage
- 9.7 Configuration Management Procedures
- 9.8 Software Accountability

10.0 Manage Problems and Incidents

- 10.1 Problem Management System
- 10.2 Problem Escalation
- 10.3 Problem Tracking and Audit Trail
- 10.4 Emergency and Temporary Access Authorisations
- 10.5 Emergency Processing Priorities

11.0 Manage Data

- 11.1 Data Preparation Procedures
- 11.2 Source Document Authorisation Procedures
- 11.3 Source Document Data Collection
- 11.4 Source Document Error Handling
- 11.5 Source Document Retention
- 11.6 Data Input Authorisation Procedures
- 11.7 Accuracy, Completeness and Authorisation Checks
- 11.8 Data Input Error Handling
- 11.9 Data Processing Integrity

DOMAINS, PROCESSES AND CONTROL OBJECTIVES

- 11.10 Data Processing Validation and Editing
- 11.11 Data Processing Error Handling
- 11.12 Output Handling and Retention
- 11.13 Output Distribution
- 11.14 Output Balancing and Reconciliation
- 11.15 Output Review and Error Handling
- 11.16 Security Provision for Output Reports
- 11.17 Protection of Sensitive Information During Transmission and Transport
- 11.18 Protection of Disposed Sensitive Information
- 11.19 Storage Management
- 11.20 Retention Periods and Storage Terms
- 11.21 Media Library Management System
- 11.22 Media Library Management Responsibilities
- 11.23 Back-up and Restoration
- 11.24 Back-up Jobs
- 11.25 Back-up Storage
- 11.26 Archiving
- 11.27 Protection of Sensitive Messages
- 11.28 Authentication and Integrity
- 11.29 Electronic Transaction Integrity
- 11.30 Continued Integrity of Stored Data

12.0 Manage Facilities

- 12.1 Physical Security
- 12.2 Low Profile of the IT Site
- 12.3 Visitor Escort
- 12.4 Personnel Health and Safety
- 12.5 Protection Against Environmental Factors
- 12.6 Uninterruptible Power Supply

13.0 Manage Operations

- 13.1 Processing Operations Procedures and Instructions Manual
- 13.2 Start-up Process and Other Operations Documentation
- 13.3 Job Scheduling
- 13.4 Departures from Standard Job Schedules
- 13.5 Processing Continuity
- 13.6 Operations Logs
- 13.7 Safeguard Special Forms and Output Devices
- 13.8 Remote Operations

MONITORING

1.0 Monitor the Processes

- 1.1 Collecting Monitoring Data
- 1.2 Assessing Performance
- 1.3 Assessing Customer Satisfaction
- 1.4 Management Reporting

2.0 Assess Internal Control Adequacy

- 2.1 Internal Control Monitoring
- 2.2 Timely Operation of Internal Controls
- 2.3 Internal Control Level Reporting
- 2.4 Operational Security and Internal Control Assurance

3.0 Obtain Independent Assurance

- 3.1 Independent Security and Internal Control Certification/Accreditation of IT Services
- 3.2 Independent Security and Internal Control Certification/Accreditation of Third-Party Service Providers
- 3.3 Independent Effectiveness Evaluation of IT Services
- 3.4 Independent Effectiveness Evaluation of Third-Party Service Providers
- 3.5 Independent Assurance of Compliance with Laws and Regulatory Requirements and Contractual Commitments
- 3.6 Independent Assurance of Compliance with Laws and Regulatory Requirements and Contractual Commitments by Third-Party Service Providers
- 3.7 Competence of Independent Assurance Function
- 3.8 Proactive Audit Involvement

4.0 Provide for Independent Audit

- 4.1 Audit Charter
- 4.2 Independence
- 4.3 Professional Ethics and Standards
- 4.4 Competence
- 4.5 Planning
- 4.6 Performance of Audit Work
- 4.7 Reporting
- 4.8 Follow-up Activities

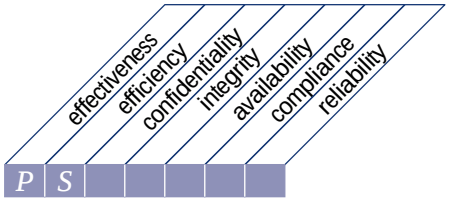
This page intentionally left blank

CONTROL OBJECTIVES

This page intentionally left blank

PLANNING & ORGANISATION

HIGH-LEVEL CONTROL OBJECTIVE



Control over the IT process of

defining a strategic IT plan

that satisfies the business requirement

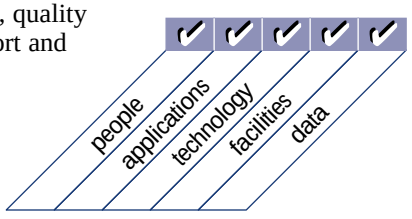
to strike an optimum balance of information technology opportunities and IT business requirements as well as ensuring its further accomplishment

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, quality
- need for senior management buy-in, support and critical review



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 which 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 which 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 re-engineering, staffing, in- or out-sourcing, 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 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

DETAILED CONTROL OBJECTIVES *continued*

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.

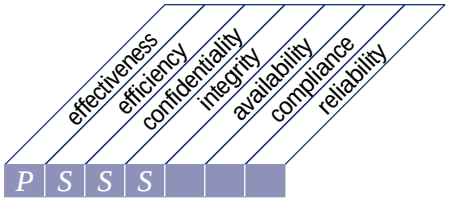
1.8 **Assessment of Existing Systems**

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 in order to determine the degree to which the existing systems support the organisation's business requirements.

This page intentionally left blank

HIGH-LEVEL CONTROL OBJECTIVE



Control over the IT process of

defining the information architecture

that satisfies the business requirement

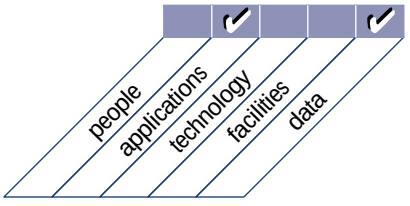
of optimising the organisation of the information systems

is enabled by

creating and maintaining a business information model and ensuring appropriate systems are defined to optimise the use of this information

and takes into consideration

- automated data repository and dictionary
- data syntax rules
- data ownership and criticality/security classification
- an information model representing the business
- enterprise information architectural standards



DETAILED CONTROL OBJECTIVES

2 DEFINE THE INFORMATION ARCHITECTURE

2.1 Information Architecture Model

CONTROL OBJECTIVE

Information should be kept consistent with needs and should be identified, captured and communicated in a form and timeframe that enables people to carry out their responsibilities effectively and on a timely basis. Accordingly, the IT function should create and regularly update an information architecture model, encompassing the corporate data model and the associated information systems. The information architecture model should be kept consistent with the IT long-range plan.

2.2 Corporate Data Dictionary and Data Syntax Rules

CONTROL OBJECTIVE

The IT function should ensure the creation and continuous updating of a corporate data dictionary which incorporates the organisation's data syntax rules.

2.3 Data Classification Scheme

CONTROL OBJECTIVE

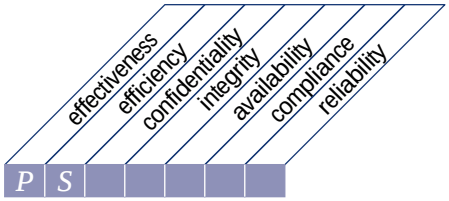
A general classification framework should be established with regard to placement of data in information classes (i.e., security categories) as well as allocation of ownership. The access rules for the classes should be appropriately defined.

2.4 Security Levels

CONTROL OBJECTIVE

Management should define, implement and maintain security levels for each of the data classifications identified above the level of "no protection required." These security levels should represent the appropriate (minimum) set of security and control measures for each of the classifications and should be re-evaluated periodically and modified accordingly. Criteria for supporting different levels of security in the extended enterprise should be established to address the needs of evolving e-commerce, mobile computing and telecommuting environments.

HIGH-LEVEL CONTROL OBJECTIVE



Control over the IT process of

determining technological direction

that satisfies the business requirement

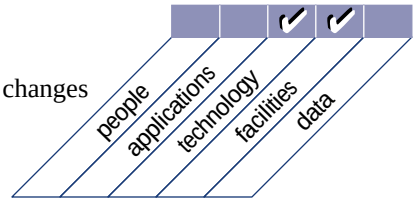
to take advantage of available and emerging technology to drive and make possible the business strategy

is enabled by

creation and maintenance of a technological infrastructure plan that sets and manages clear and realistic expectations of what technology can offer in terms of products, services and delivery mechanisms

and takes into consideration

- capability of current infrastructure
- monitoring technology developments via reliable sources
- conducting proof-of-concepts
- risk, constraints and opportunities
- acquisition plans
- migration strategy and roadmaps
- vendor relationships
- independent technology reassessment
- hardware and software price/performance changes



DETAILED CONTROL OBJECTIVES

3 DETERMINE TECHNOLOGICAL DIRECTION

3.1 Technological Infrastructure Planning

CONTROL OBJECTIVE

The IT function should create and regularly update a technological infrastructure plan which is in accordance with the IT long- and short-range plans. Such a plan should encompass aspects such as systems architecture, technological direction and migration strategies.

3.2 Monitor Future Trends and Regulations

CONTROL OBJECTIVE

Continuous monitoring of future trends and regulatory conditions should be ensured by the IT function so that these factors can be taken into consideration during the development and maintenance of the technological infrastructure plan.

3.3 Technological Infrastructure Contingency

CONTROL OBJECTIVE

The technological infrastructure plan should be assessed systematically for contingency aspects (i.e., redundancy, resilience, adequacy and evolutionary capability of the infrastructure).

3.4 Hardware and Software Acquisition Plans

CONTROL OBJECTIVE

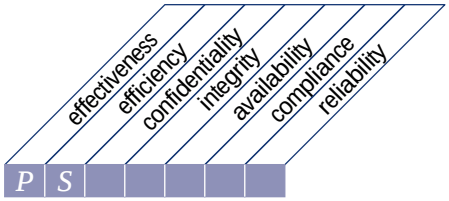
IT management should ensure that hardware and software acquisition plans are established and reflect the needs identified in the technological infrastructure plan.

3.5 Technology Standards

CONTROL OBJECTIVE

Based on the technological infrastructure plan, IT management should define technology norms in order to foster standardisation.

HIGH-LEVEL CONTROL OBJECTIVE



Control over the IT process of

defining the IT organisation and relationships

that satisfies the business requirement

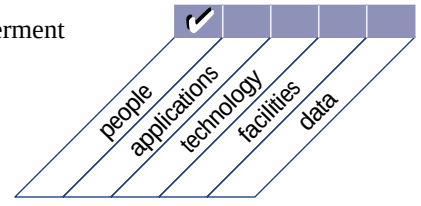
to deliver the right IT services

is enabled by

an organisation suitable in numbers and skills with roles and responsibilities defined and communicated, aligned with the business and that facilitates the strategy and provides for effective direction and adequate control

and takes into consideration

- board level responsibility for IT
- management's direction and supervision of IT
- IT's alignment with the business
- IT's involvement in key decision processes
- organisational flexibility
- clear roles and responsibilities
- balance between supervision and empowerment
- job descriptions
- staffing levels and key personnel
- organisational positioning of security, quality and internal control functions
- segregation of duties



DETAILED CONTROL OBJECTIVES

4 DEFINE THE INFORMATION TECHNOLOGY ORGANISATION AND RELATIONSHIPS

4.1 IT Planning or Steering Committee

CONTROL OBJECTIVE

The organisation's senior management should appoint a planning or steering committee to oversee the IT function and its activities. Committee membership should include representatives from senior management, user management and the IT function. The committee should meet regularly and report to senior management.

4.2 Organisational Placement of the IT Function

CONTROL OBJECTIVE

In placing the IT function in the overall organisation structure, senior management should ensure authority, critical mass and independence from user departments to the degree necessary to guarantee effective IT solutions and sufficient progress in implementing them, and to establish a partnership relation with top management to help increase awareness, understanding and skill in identifying and resolving IT issues.

4.3 Review of Organisational Achievements

CONTROL OBJECTIVE

A framework should be in place for reviewing the organisational structure to continuously meet objectives and changing circumstances.

4.4 Roles and Responsibilities

CONTROL OBJECTIVE

Management should ensure that all personnel in the organisation have and know their roles and responsibilities in relation to information systems. All personnel should have sufficient authority to exercise the role and responsibility assigned to them. Roles should be designed with consideration to appropriate segregation of duties. No one individual should control all key aspects of a transaction or event. Everyone should be made aware that they have some degree of responsibility for internal control and security. Consequently, regular campaigns should be organised and undertaken to increase awareness and discipline.

4.5 Responsibility for Quality Assurance

CONTROL OBJECTIVE

Management should assign the responsibility for the performance of the quality assurance function to staff members of the IT function and ensure that appropriate quality assurance, systems, controls and communications expertise exist in the IT function's quality assurance group. The organisational placement within the IT function and the responsibilities and the size of the quality assurance group should satisfy the requirements of the organisation.

4.6 Responsibility for Logical and Physical Security

CONTROL OBJECTIVE

Management should formally assign the responsibility for assuring both the logical and physical security of the organisation's information assets to an information security manager, reporting to the organisation's senior management. At a minimum, security management responsibility should be established at the organisation-wide level to deal with overall security issues in an organisation. If needed, additional security management responsibilities should be assigned at a system-specific level to cope with the related security issues.

4.7 Ownership and Custodianship

CONTROL OBJECTIVE

Management should create a structure for formally appointing the data owners and custodians. Their roles and responsibilities should be clearly defined.

continued on next page

DETAILED CONTROL OBJECTIVES *continued*

4.8 **Data and System Ownership**
CONTROL OBJECTIVE
Management should ensure that all information assets (data and systems) have an appointed owner who makes decisions about classification and access rights. System owners typically delegate day-to-day custodianship to the systems delivery/operations group and delegate security responsibilities to a security administrator. Owners, however, remain accountable for the maintenance of appropriate security measures.

4.9 **Supervision**
CONTROL OBJECTIVE
Senior management should implement adequate supervisory practices in the IT function to ensure that roles and responsibilities are properly exercised, to assess whether all personnel have sufficient authority and resources to execute their roles and responsibilities, and to generally review key performance indicators.

4.10 **Segregation of Duties**
CONTROL OBJECTIVE
Senior management should implement a division of roles and responsibilities which should exclude the possibility for a single individual to subvert a critical process. Management should also make sure that personnel are performing only those duties stipulated for their respective jobs and positions. In particular, a segregation of duties should be maintained between the following functions:
- information systems use
- data entry
- computer operation
- network management
- system administration
- systems development and maintenance
- change management
- security administration
- security audit

4.11 **IT Staffing**
CONTROL OBJECTIVE
Staffing requirements evaluations should be performed regularly to ensure the IT function has a sufficient number of competent IT staff. Staffing requirements should be evaluated at least annually or upon major changes to the business, operational or IT environment. Evaluation results should be acted upon promptly to ensure adequate staffing now and in the future.

4.12 **Job or Position Descriptions for IT Staff**
CONTROL OBJECTIVE
Management should ensure that position descriptions for IT staff are established and updated regularly. These position descriptions should clearly delineate both authority and responsibility, include definitions of skills and experience needed in the relevant position, and be suitable for use in performance evaluation.

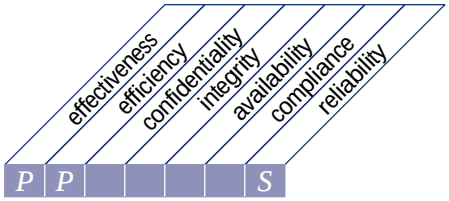
4.13 **Key IT Personnel**
CONTROL OBJECTIVE
IT management should define and identify key IT personnel.

4.14 **Contracted Staff Policies and Procedures**
CONTROL OBJECTIVE
Management should define and implement relevant policies and procedures for controlling the activities of consultants and other contract personnel by the IT function to assure the protection of the organisation's information assets.

4.15 **Relationships**
CONTROL OBJECTIVE
IT management should undertake the necessary actions to establish and maintain an optimal coordination, communication and liaison structure between the IT function and various other interests inside and outside the IT function (i.e., users, suppliers, security officers, risk managers).

This page intentionally left blank

HIGH-LEVEL CONTROL OBJECTIVE



Control over the IT process of

managing the IT investment

that satisfies the business requirement

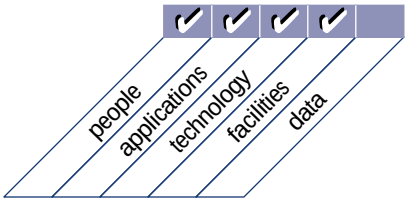
to ensure funding and to control disbursement of financial resources

is enabled by

a periodic investment and operational budget established and approved by the business

and takes into consideration

- funding alternatives
- clear budget ownership
- control of actual spending
- cost justification and awareness of total cost of ownership
- benefit justification and accountability for benefit fulfillment
- technology and application software life cycles
- alignment with enterprise business strategy
- impact assessment
- asset management



DETAILED CONTROL OBJECTIVES

5 MANAGE THE INFORMATION TECHNOLOGY INVESTMENT

5.1 Annual IT Operating Budget

CONTROL OBJECTIVE

Senior management should implement a budgeting process to ensure that an annual IT operating budget is established and approved in line with the organisation's long- and short-range plans as well as with the IT long- and short-range plans. Funding alternatives should be investigated.

5.2 Cost and Benefit Monitoring

CONTROL OBJECTIVE

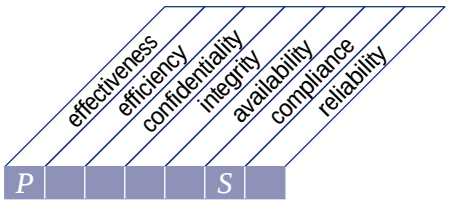
Management should establish a cost monitoring process comparing actuals to budgets. Moreover, the possible benefits derived from the IT activities should be determined and reported. For cost monitoring, the source of the actual figures should be based upon the organisation's accounting system and that system should routinely record, process and report the costs associated with the activities of the IT function. For benefit monitoring, high-level performance indicators should be defined, regularly reported and reviewed for adequacy.

5.3 Cost and Benefit Justification

CONTROL OBJECTIVE

A management control should be in place to guarantee that the delivery of services by the IT function is cost justified and in line with the industry. The benefits derived from IT activities should similarly be analysed.

HIGH-LEVEL CONTROL OBJECTIVE



Control over the IT process of

communicating management aims and direction

that satisfies the business requirement

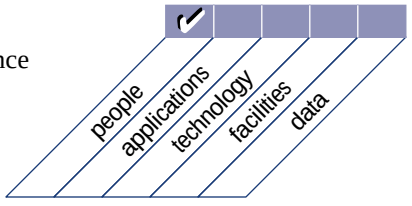
to ensure user awareness and understanding of those aims

is enabled by

policies established and communicated to the user community; furthermore, standards need to be established to translate the strategic options into practical and usable user rules

and takes into consideration

- clearly articulated mission
- technology directives linked to business aims
- code of conduct/ethics
- quality commitment
- security and internal control policies
- security and internal control practices
- lead-by-example
- continuous communications programme
- providing guidance and checking compliance



DETAILED CONTROL OBJECTIVES

6 COMMUNICATE MANAGEMENT AIMS AND DIRECTION

6.1 Positive Information Control Environment

CONTROL OBJECTIVE

In order to provide guidance for proper behaviour, remove temptation for unethical behaviour and provide discipline, where appropriate, management should create a framework and an awareness programme fostering a positive control environment throughout the entire organisation. This should address the integrity, ethical values and competence of the people, management philosophy, operating style and accountability. Specific attention is to be given to IT aspects, including security and business continuity planning.

6.2 Management's Responsibility for Policies

CONTROL OBJECTIVE

Management should assume full responsibility for formulating, developing, documenting, promulgating and controlling policies covering general aims and directives. Regular reviews of policies for appropriateness should be carried out. The complexity of the written policies and procedures should always be commensurate with the organisation size and management style.

6.3 Communication of Organisation Policies

CONTROL OBJECTIVE

Management should ensure that organisational policies are clearly communicated, understood and accepted by all levels in the organisation. The communication process should be supported by an effective plan that uses a diversified set of communication means.

6.4 Policy Implementation Resources

CONTROL OBJECTIVE

Management should plan for appropriate resources for policy implementation and for ensuring compliance, so that they are built into and are an integral part of operations. Management should also monitor the timeliness of the policy implementation.

6.5 Maintenance of Policies

CONTROL OBJECTIVE

Policies should be adjusted regularly to accommodate changing conditions. Policies should be re-evaluated, at least annually or upon significant changes to the operating or business environment, to assess their adequacy and appropriateness, and amended as necessary. Management should provide a framework and process for the periodic review and approval of standards, policies, directives and procedures.

6.6 Compliance with Policies, Procedures and Standards

CONTROL OBJECTIVE

Management should ensure that appropriate procedures are in place to determine whether personnel understand the implemented policies and procedures, and that the polices and procedures are being followed. Compliance procedures for ethical, security and internal control standards should be set by top management and promoted by example.

6.7 Quality Commitment

CONTROL OBJECTIVE

IT management should define, document and maintain a quality philosophy, policies and objectives which are consistent with the corporate philosophies and policies in this regard. The quality philosophy, policies and objectives should be understood, implemented and maintained at all levels of the IT function.

continued on next page

DETAILED CONTROL OBJECTIVES *continued*

6.8 **Security and Internal Control Framework Policy**
CONTROL OBJECTIVE
Management should assume full responsibility for developing and maintaining a framework policy which establishes the organisation's overall approach to security and internal control to establish and improve the protection of IT resources and integrity of IT systems. The policy should comply with overall business objectives and be aimed at minimisation of risks through preventive measures, timely identification of irregularities, limitation of losses and timely restoration. Measures should be based on cost/benefit analyses and should be prioritised. In addition, management should ensure that this high-level security and internal control policy specifies the purpose and objectives, the management structure, the scope within the organisation, the definition and assignment of responsibilities for implementation at all levels, and the definition of penalties and disciplinary actions associated with failing to comply with security and internal control policies. Criteria for periodic re-evaluation of the framework should be defined to support responsiveness to changing organisational, environmental and technical requirements.

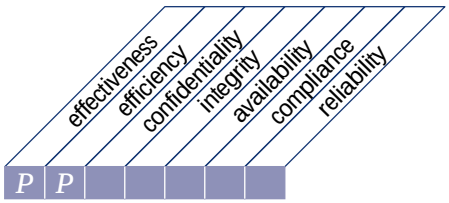
6.9 **Intellectual Property Rights**
CONTROL OBJECTIVE
Management should provide and implement a written policy on intellectual property rights covering in-house as well as contract-developed software.

6.10 **Issue-Specific Policies**
CONTROL OBJECTIVE
Measures should be put in place to ensure that issue-specific policies are established to document management decisions in addressing particular activities, applications, systems or technologies.

6.11 **Communication of IT Security Awareness**
CONTROL OBJECTIVE
An IT security awareness programme should communicate the IT security policy to each IT user and assure a complete understanding of the importance of IT security. It should convey the message that IT security is to the benefit of the organisation, all its employees, and that everybody is responsible for it. The IT security awareness programme should be supported by, and represent, the view of management.

This page intentionally left blank

HIGH-LEVEL CONTROL OBJECTIVE



Control over the IT process of

managing human resources

that satisfies the business requirement

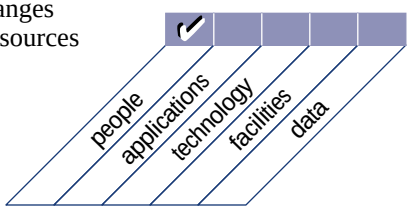
to acquire and maintain a motivated and competent workforce and maximise personnel contributions to the IT processes

is enabled by

sound, fair and transparent personnel management practices to recruit, line, vet, compensate, train, appraise, promote and dismiss

and takes into consideration

- recruitment and promotion
- training and qualification requirements
- awareness building
- cross-training and job rotation
- hiring, vetting and dismissal procedures
- objective and measurable performance evaluation
- responsiveness to technical and market changes
- properly balancing internal and external resources
- succession plan for key positions



DETAILED CONTROL OBJECTIVES

7 MANAGE HUMAN RESOURCES

7.1 Personnel Recruitment and Promotion

CONTROL OBJECTIVE

Management should implement and regularly assess the needed processes to ensure that personnel recruiting and promotion practices are based on objective criteria and consider education, experience and responsibility. These processes should be in line with the overall organisation's policies and procedures in this regard, such as hiring, orienting, training, evaluating, counselling, promoting, compensating and disciplining. Management should ensure that knowledge and skill needs are continually assessed and that the organisation is able to obtain a workforce that has the skills which match those necessary to achieve organisational goals.

7.2 Personnel Qualifications

CONTROL OBJECTIVE

IT management should regularly verify that personnel performing specific tasks are qualified on the basis of appropriate education, training and/or experience, as required. Management should encourage personnel to obtain membership in professional organisations.

7.3 Roles and Responsibilities

CONTROL OBJECTIVE

Management should clearly define roles and responsibilities for personnel, including the requirement to adhere to management policies and procedures, the code of ethics and professional practices. The terms and conditions of employment should stress the employee's responsibility for information security and internal control.

7.4 Personnel Training

CONTROL OBJECTIVE

Management should ensure that employees are provided with orientation upon hiring and with on-going training to maintain their knowledge, skills, abilities and security awareness to the level required to perform effectively. Education and training programmes conducted to effectively raise the technical and management skill levels of personnel should be reviewed regularly.

7.5 Cross-Training or Staff Back-up

CONTROL OBJECTIVE

Management should provide for sufficient cross-training or back-up of identified key personnel to address unavailabilities. Management should establish succession plans for all key functions and positions. Personnel in sensitive positions should be required to take uninterrupted holidays of sufficient length to exercise the organisation's ability to cope with unavailabilities and to prevent and detect fraudulent activity.

7.6 Personnel Clearance Procedures

CONTROL OBJECTIVE

IT management should ensure that their personnel are subjected to security clearance before they are hired, transferred or promoted, depending on the sensitivity of the position. An employee who was not subjected to such a clearance when first hired, should not be placed in a sensitive position until a security clearance has been obtained.

continued on next page

DETAILED CONTROL OBJECTIVES *continued*

7.7 **Employee Job Performance Evaluation**

CONTROL OBJECTIVE

Management should implement an employee performance evaluation process, reinforced by an effective reward system, that is designed to help employees understand the connection between their performance and the organisation's success. Evaluation should be performed against established standards and specific job responsibilities on a regular basis. Employees should receive counselling on performance or conduct whenever appropriate.

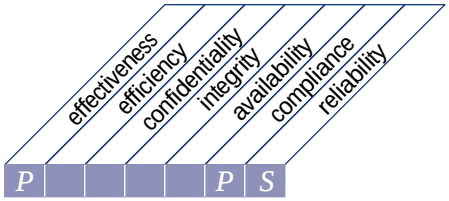
7.8 **Job Change and Termination**

CONTROL OBJECTIVE

Management should ensure that appropriate and timely actions are taken regarding job changes and job terminations so that internal controls and security are not impaired by such occurrences.

This page intentionally left blank

HIGH-LEVEL CONTROL OBJECTIVE



Control over the IT process of

ensuring compliance with external requirements

that satisfies the business requirement

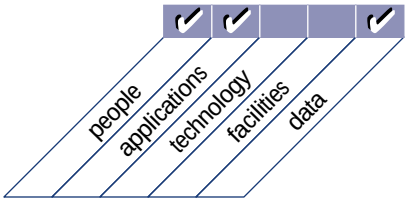
to meet legal, regulatory and contractual obligations

is enabled by

identifying and analysing external requirements for their IT impact, and taking appropriate measures to comply with them

and takes into consideration

- laws, regulations and contracts
- monitoring legal and regulatory developments
- regular monitoring for compliance
- safety and ergonomics
- privacy
- intellectual property



DETAILED CONTROL OBJECTIVES

8 ENSURE COMPLIANCE WITH EXTERNAL REQUIREMENTS

8.1 External Requirements Review

CONTROL OBJECTIVE

The organisation should establish and maintain procedures for external requirements review and for the coordination of these activities. Continuous research should determine the applicable external requirements for the organisation. Legal, government or other external requirements related to IT practices and controls should be reviewed. Management should also assess the impact of any external relationships on the organisation's overall information needs, including determination of the extent to which IT strategies need to conform with or support the requirements of any related third-parties.

8.2 Practices and Procedures for Complying with External Requirements

CONTROL OBJECTIVE

Organisational practices should ensure that appropriate corrective actions are taken on a timely basis to guarantee compliance with external requirements. In addition, adequate procedures assuring continuous compliance should be established and maintained. In this regard, management should seek legal advice if required.

8.3 Safety and Ergonomic Compliance

CONTROL OBJECTIVE

Management should ensure compliance with safety and ergonomic standards in the working environment of IT users and personnel.

8.4 Privacy, Intellectual Property and Data Flow

CONTROL OBJECTIVE

Management should ensure compliance with privacy, intellectual property, transborder data flow and cryptographic regulations applicable to the IT practices of the organisation.

8.5 Electronic Commerce

CONTROL OBJECTIVE

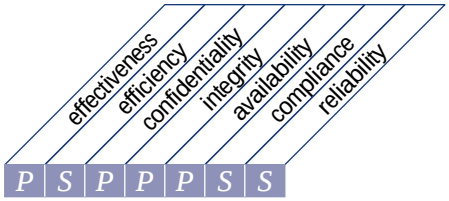
Management should ensure that formal contracts are in place establishing agreement between trading partners on communication processes and on standards for transaction message security and data storage. When trading on the Internet, management should enforce adequate controls to ensure compliance with local laws and customs on a world-wide basis.

8.6 Compliance with Insurance Contracts

CONTROL OBJECTIVE

Management should ensure that insurance contract requirements are properly identified and continuously met.

HIGH-LEVEL CONTROL OBJECTIVE



Control over the IT process of

assessing risks

that satisfies the business requirement

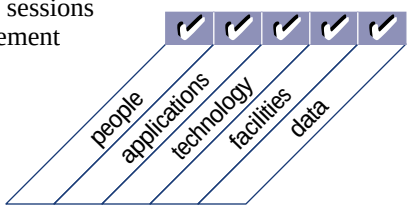
of supporting management decisions through achieving IT objectives and responding to threats by reducing complexity, increasing objectivity and identifying important decision factors

is enabled by

the organisation engaging itself in IT risk-identification and impact analysis, involving multi-disciplinary 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



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 which 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

DETAILED CONTROL OBJECTIVES *continued*

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 needs to balance prevention, detection, correction and recovery measures. Furthermore, management needs to communicate the purpose of the control measures, manage conflicting measures and monitor the continuing effectiveness of all control measures.

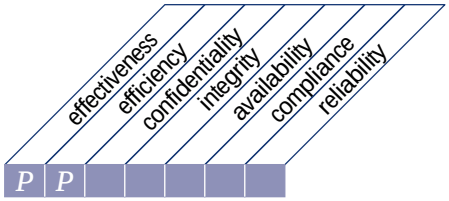
9.8 **Risk Assessment Commitment**

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.

This page intentionally left blank

HIGH-LEVEL CONTROL OBJECTIVE



Control over the IT process of

managing projects

that satisfies the business requirement

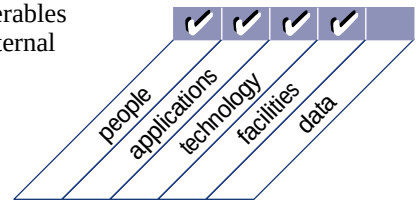
to set priorities and to deliver on time and within budget

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



DETAILED CONTROL OBJECTIVES

10 MANAGE PROJECTS

10.1 Project Management Framework

CONTROL OBJECTIVE

Management should establish a general project management framework which 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 which is adequate for maintaining control over the project throughout its life and which 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 which is then integrated with the project master plan and formally reviewed and agreed to by all parties concerned.

10.9 Planning of Assurance Methods

CONTROL OBJECTIVE

Assurance tasks are to be identified during the planning phase of the project management

continued on next page

DETAILED CONTROL OBJECTIVES *continued*

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.

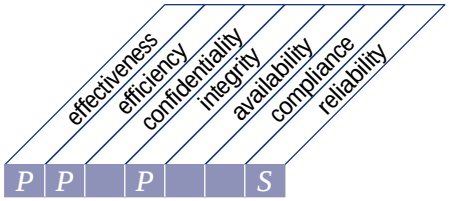
10.13 **Post-Implementation Review Plan**

CONTROL OBJECTIVE

The organisation's project management framework should provide, as an integral part of the project team's activities, for 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.

This page intentionally left blank

HIGH-LEVEL CONTROL OBJECTIVE



Control over the IT process of

managing quality

that satisfies the business requirement

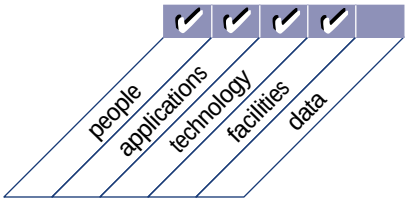
to meet the IT customer requirements

is enabled by

the planning, implementing and maintaining of quality management standards and systems providing for distinct development phases, clear deliverables and explicit responsibilities

and takes into consideration

- establishment of a quality culture
- quality plans
- quality assurance responsibilities
- quality control practices
- system development life cycle methodology
- programme and system testing and documentation
- quality assurance reviews and reporting
- training and involvement of end user and quality assurance personnel
- development of a quality assurance knowledge base
- benchmarking against industry norms



DETAILED CONTROL OBJECTIVE

11 MANAGE QUALITY

11.1 General Quality Plan

CONTROL OBJECTIVE

Management should develop and regularly maintain an overall quality plan based on the organisational and IT long-range plans. The plan should promote the continuous improvement philosophy and answer the basic questions of what, who and how.

11.2 Quality Assurance Approach

CONTROL OBJECTIVE

Management should establish a standard approach regarding quality assurance which covers both general and project specific quality assurance activities. The approach should prescribe the type(s) of quality assurance activities (such as reviews, audits, inspections, etc.) to be performed to achieve the objectives of the general quality plan. It should also require specific quality assurance reviews.

11.3 Quality Assurance Planning

CONTROL OBJECTIVE

Management should implement a quality assurance planning process to determine the scope and timing of the quality assurance activities.

11.4 Quality Assurance Review of Adherence to IT Standards and Procedures

CONTROL OBJECTIVE

Management should ensure that the responsibilities assigned to the quality assurance personnel include a review of general adherence to IT standards and procedures.

11.5 System Development Life Cycle Methodology

CONTROL OBJECTIVE

The organisation's management should define and implement IT standards and adopt a system development life cycle methodology governing the process of developing, acquiring, implementing and maintaining computerised information systems and related technology. The chosen system development life cycle methodology should be appropriate for the systems to be developed, acquired, implemented and maintained.

11.6 System Development Life Cycle Methodology for Major Changes to Existing Technology

CONTROL OBJECTIVE

In the event of major changes to existing technology, management should ensure that a system development life cycle methodology is observed, as in the case of the acquisition or development of new technology.

11.7 Updating of the System Development Life Cycle Methodology

CONTROL OBJECTIVE

Management should implement a periodic review of its system development life cycle methodology to ensure that its provisions reflect current generally accepted techniques and procedures.

11.8 Coordination and Communication

CONTROL OBJECTIVE

Management should establish a process for ensuring close coordination and communication between customers of the IT function and system implementors. This process should entail structured methods using the system development life cycle methodology to ensure the provision of quality IT solutions which meet the business demands. Management should promote an organisation which is characterised by close cooperation and communication throughout the system development life cycle.

continued on next page

DETAILED CONTROL OBJECTIVES *continued*

11.9 **Acquisition and Maintenance Framework for the Technology Infrastructure**
CONTROL OBJECTIVE
A general framework should be in place regarding the acquisition and maintenance of the technology infrastructure. The different steps to be followed regarding the technology infrastructure (such as acquiring; programming, documenting, and testing; parameter setting; maintaining and applying fixes) should be governed by, and in line with, the acquisition and maintenance framework for the technology infrastructure.

11.10 **Third-Party Implementor Relationships**
CONTROL OBJECTIVE
Management should implement a process to ensure good working relationships with third-party implementors. Such a process should provide that the user and implementor agree to acceptance criteria, handling of changes, problems during development, user roles, facilities, tools, software, standards and procedures.

11.11 **Programme Documentation Standards**
CONTROL OBJECTIVE
The organisation's system development life cycle methodology should incorporate standards for programme documentation which have been communicated to the concerned staff and enforced. The methodology should ensure that the documentation created during information system development or modification projects conforms to these standards.

11.12 **Programme Testing Standards**
CONTROL OBJECTIVE
The organisation's system development life cycle methodology should provide standards covering test requirements, verification, documentation and retention for testing individual software units and aggregated programmes created as part of every information system development or modification project.

11.13 **System Testing Standards**
CONTROL OBJECTIVE
The organisation's system development life cycle methodology should provide standards covering test requirements, verification, documentation, and retention for the testing of the total system as a part of every information system development or modification project.

11.14 **Parallel/Pilot Testing**
CONTROL OBJECTIVE
The organisation's system development life cycle methodology should define the circumstances under which parallel or pilot testing of new and/or existing systems will be conducted.

11.15 **System Testing Documentation**
CONTROL OBJECTIVE
The organisation's system development life cycle methodology should provide, as part of every information system development, implementation, or modification project, that the documented results of testing the system are retained.

11.16 **Quality Assurance Evaluation of Adherence to Development Standards**

CONTROL OBJECTIVE

The organisation's quality assurance approach should require that a post-implementation review of an operational information system assess whether the project team adhered to the provisions of the system development life cycle methodology.

11.17 **Quality Assurance Review of the Achievement of IT Objectives**

CONTROL OBJECTIVE

The quality assurance approach should include a review of the extent to which particular systems and application development activities have achieved the objectives of the information services function.

11.18 **Quality Metrics**

CONTROL OBJECTIVE

Management should define and use metrics to measure the results of activities, thus assessing whether quality goals have been achieved.

11.19 **Reports of Quality Assurance Reviews**

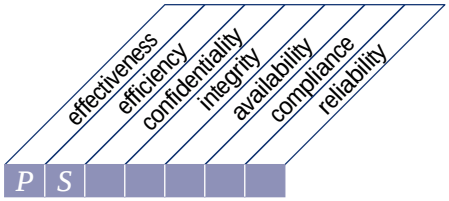
CONTROL OBJECTIVE

Reports of quality assurance reviews should be prepared and submitted to management of user departments and the IT function.

This page intentionally left blank

ACQUISITION & IMPLEMENTATION

HIGH-LEVEL CONTROL OBJECTIVE



Control over the IT process of

identifying automated solutions

that satisfies the business requirement

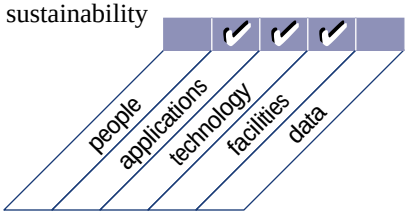
of ensuring an effective and efficient approach to satisfy the user requirements

is enabled by

an objective and clear identification and analysis of the alternative opportunities measured against user requirements

and takes into consideration

- knowledge of solutions available in the market
- acquisition and implementation methodologies
- user involvement and buy in
- alignment with enterprise and IT strategies
- information requirements definition
- feasibility studies (costs, benefits, alternatives, etc.)
- functionality, operability, acceptability and sustainability requirements
- compliance with information architecture
- cost-effective security and control
- supplier responsibilities



DETAILED CONTROL OBJECTIVES

1 IDENTIFY AUTOMATED SOLUTIONS

1.1 Definition of Information Requirements

CONTROL OBJECTIVE

The organisation's system development life cycle methodology should provide that the business requirements satisfied by the existing system and to be satisfied by the proposed new or modified system (software, data and infrastructure) be clearly defined before a development, implementation or modification project is approved. The system development life cycle methodology should require that the solution's functional and operational requirements be specified including performance, safety, reliability, compatibility, security and legislation.

1.2 Formulation of Alternative Courses of Action

CONTROL OBJECTIVE

The organisation's system development life cycle methodology should provide for the analysis of the alternative courses of action that will satisfy the business requirements established for a proposed new or modified system.

1.3 Formulation of Acquisition Strategy

CONTROL OBJECTIVE

Information systems acquisition, development and maintenance should be considered in the context of the organisation's IT long- and short-range plans. The organisation's system development life cycle methodology should provide for a software acquisition strategy plan defining whether the software will be acquired off-the-shelf, developed internally, through contract or by enhancing the existing software, or a combination of all these.

1.4 Third-Party Service Requirements

CONTROL OBJECTIVE

The organisation's system development life cycle methodology should provide for the evaluation of the requirements and the specifications for an RFP (request for proposal) when dealing with a third-party service vendor.

1.5 Technological Feasibility Study

CONTROL OBJECTIVE

The organisation's system development life cycle methodology should provide for an examination of the technological feasibility of each alternative for satisfying the business requirements established for the development of a proposed new or modified information system project.

1.6 Economic Feasibility Study

CONTROL OBJECTIVE

The organisation's system development life cycle methodology should provide, in each proposed information systems development, implementation and modification project, for an analysis of the costs and benefits associated with each alternative being considered for satisfying the established business requirements.

1.7 Information Architecture

CONTROL OBJECTIVE

Management should ensure that attention is paid to the enterprise data model while solutions are being identified and analysed for feasibility.

1.8 Risk Analysis Report

CONTROL OBJECTIVE

The organisation's system development life cycle methodology should provide, in each proposed information system development, implementation or modification project, for an analysis and documentation of the security threats, potential vulnerabilities and impacts, and the feasible security and internal control safeguards for reducing or eliminating the identified risk. This should be realised in line with the overall risk assessment framework.

continued on next page

DETAILED CONTROL OBJECTIVES *continued*

1.9 **Cost-Effective Security Controls**
CONTROL OBJECTIVE
Management should ensure that the costs and benefits of security are carefully examined in monetary and non-monetary terms to guarantee that the costs of controls do not exceed benefits. The decision requires formal management sign-off. All security requirements should be identified at the requirements phase of a project and justified, agreed and documented as part of the overall business case for an information system. Security requirements for business continuity management should be defined to ensure that the planned activation, fallback and resumption processes are supported by the proposed solution.

1.10 **Audit Trails Design**
CONTROL OBJECTIVE
The organisation's system development life cycle methodology should require that adequate mechanisms for audit trails are available or can be developed for the solution identified and selected. The mechanisms should provide the ability to protect sensitive data (e.g., user ID's) against discovery and misuse.

1.11 **Ergonomics**
CONTROL OBJECTIVE
Management should ensure that the information system development, implementation and change projects undertaken by the IT function pay attention to ergonomic issues associated with the introduction of automated solutions.

1.12 **Selection of System Software**
CONTROL OBJECTIVE
Management should ensure that a standard procedure is adhered to by the IT function to identify all potential system software programmes that will satisfy its operational requirements.

1.13 **Procurement Control**
CONTROL OBJECTIVE
Management should develop and implement a central procurement approach describing a common set of procedures and standards to be followed in the procurement of information technology related hardware, software and services. Products should be reviewed and tested prior to their use and the financial settlement.

1.14 **Software Product Acquisition**
CONTROL OBJECTIVE
Software product acquisition should follow the organisation's procurement policies.

1.15 **Third-Party Software Maintenance**
CONTROL OBJECTIVE
Management should require that for licensed software acquired from third-party providers, the providers have appropriate procedures to validate, protect and maintain the software product's integrity rights. Consideration should be given to the support of the product in any maintenance agreement related to the delivered product.

1.16 **Contract Application Programming**
CONTROL OBJECTIVE
The organisation's system development life cycle methodology should provide that the procurement of contract programming services be justified with a written request for services from a designated member of the IT function. The contract should stipulate that the software, documentation and other deliverables are subject to testing and review prior to acceptance. In addition, it should require that the end products of completed contract programming services be tested and reviewed according to the related standards by the IT function's quality assurance group and other concerned parties (such as users, project managers, etc.) before payment for the work and approval of the end product. Testing to be includ-

ed in contract specifications should consist of system testing, integration testing, hardware and component testing, procedure testing, load and stress testing, tuning and performance testing, regression testing, user acceptance testing and, finally, pilot testing of the total system to avoid any unexpected system failure.

1.17 **Acceptance of Facilities**

CONTROL OBJECTIVE

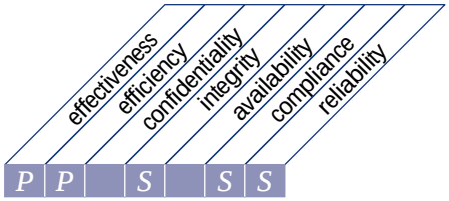
Management should ensure that an acceptance plan for facilities to be provided is agreed upon with the supplier in the contract and this plan defines the acceptance procedures and criteria. In addition, acceptance tests should be performed to guarantee that the accommodation and environment meet the requirements specified in the contract.

1.18 **Acceptance of Technology**

CONTROL OBJECTIVE

Management should ensure that an acceptance plan for specific technology to be provided is agreed upon with the supplier in the contract and this plan defines the acceptance procedures and criteria. In addition, acceptance tests provided for in the plan should include inspection, functionality tests and workload trials.

HIGH-LEVEL CONTROL OBJECTIVE



Control over the IT process of

acquiring and maintaining application software

that satisfies the business requirement

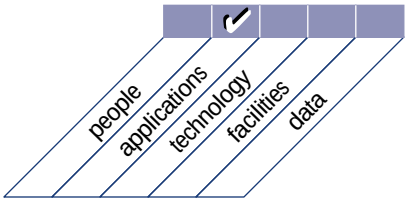
to provide automated functions which effectively support the business process

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



DETAILED CONTROL OBJECTIVES

2 ACQUIRE AND MAINTAIN APPLICATION SOFTWARE

2.1 Design Methods

CONTROL OBJECTIVE

The organisation's system development life cycle methodology should provide 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 to 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 provide that an appropriate procedure be 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 Programme Specifications

CONTROL OBJECTIVE

The organisation's system development life cycle methodology should require that detailed written programme specifications be prepared for each information system development or modification project. The methodology should further ensure that programme 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 be 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 provide 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 which is easy to use and self-documenting (by means of online help functions).

continued on next page

DETAILED CONTROL OBJECTIVES *continued*

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 which guarantee the accuracy, completeness, timeliness and authorisation of inputs, processing and outputs. Sensitivity assessment should be performed during 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 in order 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 provide 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 Programme Software**
CONTROL OBJECTIVE
The organisation should establish procedures to assure, where applicable, that application programmes contain provisions which routinely verify the tasks performed by the software to help assure data integrity, and which provide the restoration of the 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 it is approved by the user. Adequate measures should be conducted to prevent disclosure of sensitive information used during testing.

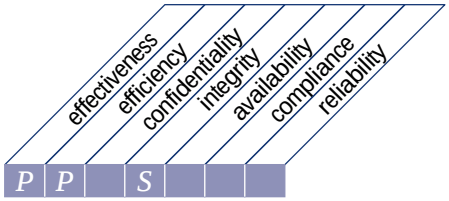
2.16 **User Reference and Support Materials**
CONTROL OBJECTIVE
The organisation's system development life cycle methodology should provide that adequate user reference and support manuals be prepared (preferably in electronic format) as part of every information system development or modification project.

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.

HIGH-LEVEL CONTROL OBJECTIVE



Control over the IT process of

acquiring and maintaining technology infrastructure

that satisfies the business requirement

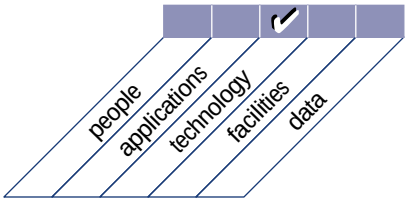
to provide the appropriate platforms for supporting business applications

is enabled by

judicious hardware and software acquisition, standardising of software, assessment of hardware and software performance, and consistent system administration

and takes into consideration

- compliance with technology infrastructure directions and standards
- technology assessment
- installation, maintenance and change controls
- upgrade, conversion and migration plans
- use of internal and external infrastructures and/or resources
- supplier responsibilities and relationships
- change management
- total cost of ownership
- system software security



DETAILED CONTROL OBJECTIVES

3 ACQUIRE AND MAINTAIN TECHNOLOGY INFRASTRUCTURE

3.1 Assessment of New Hardware and Software

CONTROL OBJECTIVE

Hardware and software selection criteria should be based on the functional specifications for the new or modified system and should identify mandatory and optional requirements. Procedures should be in place to assess new hardware and software for any impact on the performance of the overall system.

3.2 Preventative Maintenance for Hardware

CONTROL OBJECTIVE

IT management should schedule routine and periodic hardware maintenance to reduce the frequency and impact of performance failures.

3.3 System Software Security

CONTROL OBJECTIVE

IT management should ensure that the set-up of system software to be installed does not jeopardise the security of the data and programmes being stored on the system. Attention should be paid to set-up and maintenance of system software parameters.

3.4 System Software Installation

CONTROL OBJECTIVE

Procedures should be implemented to ensure that system software is installed in accordance with the acquisition and maintenance framework for the technology infrastructure. Testing should be performed before use in the production environment is authorised. A group independent of the users and developers should control the movement of programmes and data among libraries.

3.5 System Software Maintenance

CONTROL OBJECTIVE

Procedures should be implemented to ensure that system software is maintained in accordance with the acquisition and maintenance framework for the technology infrastructure.

3.6 System Software Change Controls

CONTROL OBJECTIVE

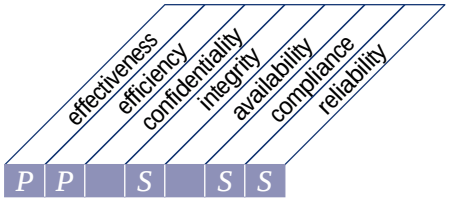
Procedures should be implemented to ensure that system software changes are controlled in line with the organisation's change management procedures.

3.7 Use and Monitoring of System Utilities

CONTROL OBJECTIVE

Policies and techniques should be implemented for using, monitoring and evaluating the use of system utilities. Responsibilities for using sensitive software utilities should be clearly defined and understood by developers, and the use of the utilities should be monitored and logged.

HIGH-LEVEL CONTROL OBJECTIVE



Control over the IT process of

developing and maintaining procedures

that satisfies the business requirement

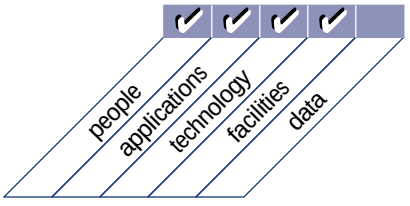
to ensure the proper use of the applications and the technological solutions put in place

is enabled by

a structured approach to the development of user and operations procedure manuals, service requirements and training materials

and takes into consideration

- business process re-design
- treating procedures as any other technology deliverable
- timely development
- user procedures and controls
- operational procedures and controls
- training materials
- managing change



DETAILED CONTROL OBJECTIVES

4 DEVELOP AND MAINTAIN PROCEDURES

4.1 Operational Requirements and Service Levels

CONTROL OBJECTIVE

The organisation's system development life cycle methodology should ensure the timely definition of operational requirements and service levels.

4.2 User Procedures Manual

CONTROL OBJECTIVE

The organisation's system development life cycle methodology should provide that adequate user procedures manuals be prepared and refreshed as part of every information system development, implementation or modification project.

4.3 Operations Manual

CONTROL OBJECTIVE

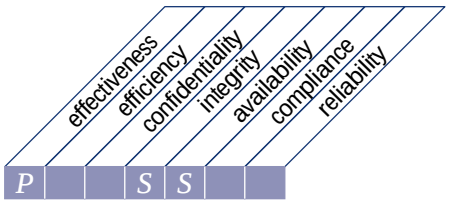
The organisation's system development life cycle methodology should provide that an adequate operations manual be prepared and kept up-to-date as part of every information system development, implementation or modification project.

4.4 Training Materials

CONTROL OBJECTIVE

The organisation's system development life cycle methodology should ensure that adequate training materials are developed as part of every information system development, implementation or modification project. These materials should be focused on the system's use in daily practice.

HIGH-LEVEL CONTROL OBJECTIVE



Control over the IT process of

installing and accrediting systems

that satisfies the business requirement

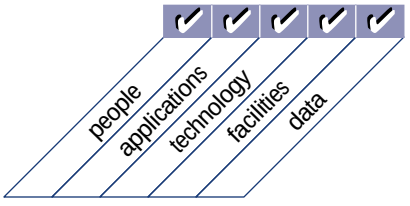
to verify and confirm that the solution is fit for the intended purpose

is enabled by

the realisation of a well-formalised installation migration, conversion and acceptance plan

and takes into consideration

- training of user and IT operations personnel
- data conversion
- a test environment reflecting the live environment
- accreditation
- post-implementation reviews and feedback
- end user involvement in testing
- continuous quality improvement plans
- business continuity requirements
- capacity and throughput measurement
- agreed upon acceptance criteria



DETAILED CONTROL OBJECTIVES

5 INSTALL AND ACCREDIT SYSTEMS

5.1 Training

CONTROL OBJECTIVE

Staff of the affected user departments and the operations group of the IT function should be trained in accordance with the defined training plan and associated materials, as part of every information systems development, implementation or modification project.

5.2 Application Software Performance Sizing

CONTROL OBJECTIVE

Application software performance sizing (optimisation) should be established as an integral part of the organisation's system development life cycle methodology to forecast the resources required for operating new and significantly changed software.

5.3 Implementation Plan

CONTROL OBJECTIVE

An implementation plan should be prepared, reviewed and approved by relevant parties and be used to measure progress. The implementation plan should address site preparation, equipment acquisition and installation, user training, installation of operating software changes, implementation of operating procedures and conversion.

5.4 System Conversion

CONTROL OBJECTIVE

The organisation's system development life cycle methodology should provide, as part of every information system development, implementation or modification project, that the necessary elements from the old system are converted to the new one according to a pre-established plan.

5.5 Data Conversion

CONTROL OBJECTIVE

Management should require that a data conversion plan is prepared, defining the methods of collecting and verifying the data to be converted and identifying and resolving any errors found during conversion. Tests to be performed include comparing the original and converted files, checking the compatibility of the converted data with the new system, checking master files after conversion to ensure the accuracy of master file data and ensuring that transactions affecting master files update both the old and the new master files during the period between initial conversion and final implementation. A detailed verification of the initial processing of the new system should be performed to confirm successful implementation. Management should ensure that the responsibility for successful conversion of data lies with the system owners.

5.6 Testing Strategies and Plans

CONTROL OBJECTIVE

Testing strategies and plans should be prepared and signed off by the system owner and IT management.

5.7 Testing of Changes

CONTROL OBJECTIVE

Management should ensure that changes are tested in accordance with the impact and resource assessment in a separate test environment by an independent (from builders) test group before use in the regular operational environment begins. Back-out plans should also be developed. Acceptance testing should be carried out in an environment representative of the future operational environment (e.g., similar security, internal controls, workloads, etc.).

5.8 Parallel/Pilot Testing Criteria and Performance

CONTROL OBJECTIVE

Procedures should be in place to ensure that parallel or pilot testing is performed in accordance with a pre-established plan and that the criteria for terminating the testing process are specified in advance.

continued on next page

DETAILED CONTROL OBJECTIVES *continued*

5.9 **Final Acceptance Test**
CONTROL OBJECTIVE
Procedures should provide, as part of the final acceptance or quality assurance testing of new or modified information systems, for a formal evaluation and approval of the test results by management of the affected user department(s) and the IT function. The tests should cover all components of the information system (e.g., application software, facilities, technology, user procedures).

5.10 **Security Testing and Accreditation**
CONTROL OBJECTIVE
Management should define and implement procedures to ensure that operations and user management formally accept the test results and the level of security for the systems, along with the remaining residual risk. These procedures should reflect the agreed upon roles and responsibilities of end user, system development, network management and system operations personnel, taking into account segregation, supervision and control issues.

5.11 **Operational Test**
CONTROL OBJECTIVE
Management should ensure that before moving the system into operation, the user or designated custodian (the party designated to run the system on behalf of the user) validates its operation as a complete product, under conditions similar to the application environment and in the manner in which the system will be run in a production environment.

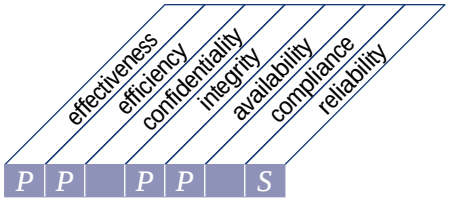
5.12 **Promotion to Production**
CONTROL OBJECTIVE
Management should define and implement formal procedures to control the handover of the system from development to testing to operations. Management should require that system owner authorisation is obtained before a new system is moved into production and that, before the old system is discontinued, the new system will have successfully operated through all daily, monthly and quarterly production cycles. The respective environments should be segregated and properly protected.

5.13 **Evaluation of Meeting User Requirements**
CONTROL OBJECTIVE
The organisation's system development life cycle methodology should require that a post-implementation review of operational information system requirements (e.g., capacity, throughput, etc.) be conducted to assess whether the users' needs are being met by the system.

5.14 **Management's Post-Implementation Review**
CONTROL OBJECTIVE
The organisation's system development life cycle methodology should require that a post-implementation review of an operational information system assess and report on whether the system delivered the benefits envisioned in the most cost effective manner.

This page intentionally left blank

HIGH-LEVEL CONTROL OBJECTIVE



Control over the IT process of

managing changes

that satisfies the business requirement

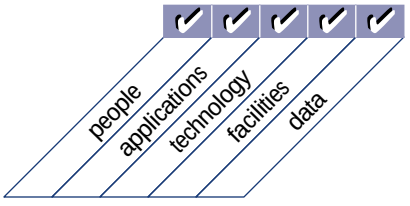
to minimise the likelihood of disruption, unauthorised alterations and errors

is enabled by

a management system which provides for the analysis, implementation and follow-up of all changes requested and made to the existing IT infrastructure

and takes into consideration

- identification of changes
- categorisation, prioritisation and emergency procedures
- impact assessment
- change authorisation
- release management
- software distribution
- use of automated tools
- configuration management
- business process re-design



DETAILED CONTROL OBJECTIVES

6 MANAGE CHANGES

6.1 Change Request Initiation and Control

CONTROL OBJECTIVE

IT management should ensure that all requests for changes, system maintenance and supplier maintenance are standardised and are subject to formal change management procedures. Changes should be categorised and prioritised and specific procedures should be in place to handle urgent matters. Change requestors should be kept informed about the status of their request.

6.2 Impact Assessment

CONTROL OBJECTIVE

A procedure should be in place to ensure that all requests for change are assessed in a structured way for all possible impacts on the operational system and its functionality.

6.3 Control of Changes

CONTROL OBJECTIVE

IT management should ensure that change management and software control and distribution are properly integrated with a comprehensive configuration management system. The system used to monitor changes to application systems should be automated to support the recording and tracking of changes made to large, complex information systems.

6.4 Emergency Changes

CONTROL OBJECTIVE

IT management should establish parameters defining emergency changes and procedures to control these changes when they circumvent the normal process of technical, operational and management assessment prior to implementation. The emergency changes should be recorded and authorised by IT management prior to implementation.

6.5 Documentation and Procedures

CONTROL OBJECTIVE

The change process should ensure that whenever system changes are implemented, the associated documentation and procedures are updated accordingly.

6.6 Authorised Maintenance

CONTROL OBJECTIVE

IT management should ensure maintenance personnel have specific assignments and that their work is properly monitored. In addition, their system access rights should be controlled to avoid risks of unauthorised access to automated systems.

6.7 Software Release Policy

CONTROL OBJECTIVE

IT management should ensure that the release of software is governed by formal procedures ensuring sign-off, packaging, regression testing, handover, etc.

6.8 Distribution of Software

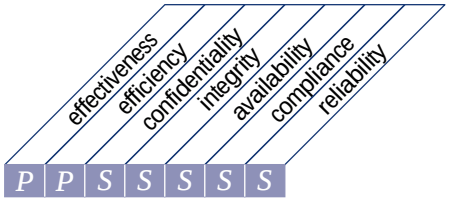
CONTROL OBJECTIVE

Specific internal control measures should be established to ensure distribution of the correct software element to the right place, with integrity, and in a timely manner with adequate audit trails.

This page intentionally left blank

DELIVERY & SUPPORT

HIGH-LEVEL CONTROL OBJECTIVE



Control over the IT process of

defining and managing service levels

that satisfies the business requirement

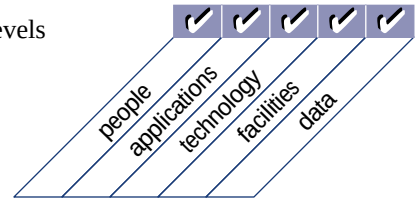
to establish a common understanding of the level of service required

is enabled by

the establishment of service-level agreements which formalise the performance criteria against which the quantity and quality of service will be measured

and takes into consideration

- formal agreements
- definition of responsibilities
- response times and volumes
- charging
- integrity guarantees
- non-disclosure agreements
- customer satisfaction criteria
- cost/benefit analysis of required service levels
- monitoring and reporting



DETAILED CONTROL OBJECTIVES

1 DEFINE AND MANAGE SERVICE LEVELS

1.1 Service Level Agreement Framework

CONTROL OBJECTIVE

Management should define a framework wherein it promotes the definition of formal service level agreements and defines the minimal contents: availability, reliability, performance, capacity for growth, levels of support provided to users, continuity planning, security, minimum acceptable level of satisfactorily delivered system functionality, restrictions (limits on the amount of work), service charges, central print facilities (availability), central print distribution and change procedures. Users and the IT function should have a written agreement which describes the service level in qualitative and quantitative terms. The agreement defines the responsibilities of both parties. The IT function must offer the agreed quality and quantity of service and the users must constrain the demands they place upon the service within the agreed limits.

1.2 Aspects of Service Level Agreements

CONTROL OBJECTIVE

Explicit agreement should be reached on the aspects that a service level agreement should have. The service level agreement should cover at least the following aspects: availability, reliability, performance, capacity for growth, levels of support provided to users, continuity planning, security, minimum acceptable level of satisfactorily delivered system functionality, restrictions (limits on the amount of work), service charges, central print facilities (availability), central print distribution and change procedures.

1.3 Performance Procedures

CONTROL OBJECTIVE

Procedures should be put in place to ensure that the manner of and responsibilities for performance governing relations (e.g., non-disclosure agreements) between all the involved parties are established, coordinated, maintained and communicated to all affected departments.

1.4 Monitoring and Reporting

CONTROL OBJECTIVE

Management should appoint a service level manager who is responsible for monitoring and reporting on the achievement of the specified service performance criteria and all problems encountered during processing. The monitoring statistics should be analysed on a timely basis. Appropriate corrective action should be taken and failures should be investigated.

1.5 Review of Service Level Agreements and Contracts

CONTROL OBJECTIVE

Management should implement a regular review process for service level agreements and underpinning contracts with third-party service providers.

1.6 Chargeable Items

CONTROL OBJECTIVE

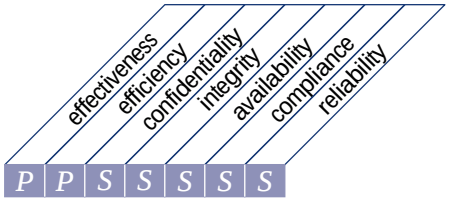
Provisions for chargeable items should be included in the service level agreements to make trade-offs possible on service levels versus costs.

1.7 Service Improvement Programme

CONTROL OBJECTIVE

Management should implement a process to ensure that users and service level managers regularly agree on a service improvement programme for pursuing cost-justified improvements to the service level.

HIGH-LEVEL CONTROL OBJECTIVE



Control over the IT process of

managing third-party services

that satisfies the business requirement

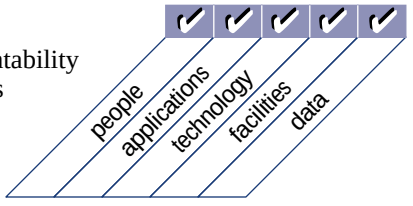
to ensure that roles and responsibilities of third parties are clearly defined, adhered to and continue to satisfy requirements

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
- non-disclosure 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 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 that 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

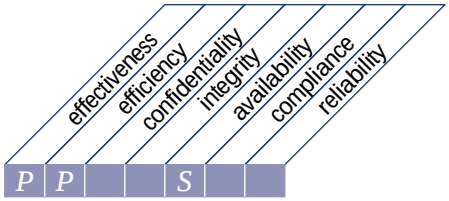
With regard to relationships with third-party service providers, management should ensure that security agreements (e.g., non-disclosure agreements) are identified and explicitly stated and agreed to, and conform to universal business standards in accordance with legal and regulatory requirements, including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

2.8 Monitoring

CONTROL OBJECTIVE

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

HIGH-LEVEL CONTROL OBJECTIVE



Control over the IT process of

managing performance and capacity

that satisfies the business requirement

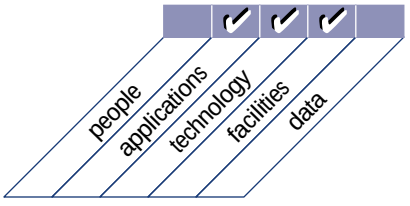
to ensure that adequate capacity is available and that best and optimal use is made of it to meet required performance needs

is enabled by

data collection, analysis and reporting on resource performance, application sizing and workload demand

and takes into consideration

- availability and performance requirements
- automated monitoring and reporting
- modeling tools
- capacity management
- resource availability
- hardware and software price/performance changes



DETAILED CONTROL OBJECTIVES

3 MANAGE PERFORMANCE AND CAPACITY

3.1 Availability and Performance Requirements

CONTROL OBJECTIVE

The management process should ensure that business needs are identified regarding availability and performance of information services and converted into availability terms and requirements.

3.2 Availability Plan

CONTROL OBJECTIVE

Management should ensure the establishment of an availability plan to achieve, monitor and control the availability of information services.

3.3 Monitoring and Reporting

CONTROL OBJECTIVE

Management should implement a process to ensure that the performance of IT resources is continuously monitored and exceptions are reported in a timely and comprehensive manner.

3.4 Modeling Tools

CONTROL OBJECTIVE

IT management should ensure that appropriate modeling tools are used to produce a model of the current system which has been calibrated and adjusted against actual workload and is accurate within recommended load levels. Modeling tools should be used to assist with the prediction of capacity, configuration reliability, performance and availability requirements. In-depth technical investigations should be conducted on systems hardware and should include forecasts concerning future technologies.

3.5 Proactive Performance Management

CONTROL OBJECTIVE

The performance management process should include forecasting capability to enable problems to be corrected before they affect system performance. Analysis should be conducted on system failures and irregularities pertaining to frequency, degree of impact and amount of damage.

3.6 Workload Forecasting

CONTROL OBJECTIVE

Controls are to be in place to ensure that workload forecasts are prepared to identify trends and to provide information needed for the capacity plan.

3.7 Capacity Management of Resources

CONTROL OBJECTIVE

IT management should establish a planning process for the review of hardware performance and capacity to ensure that cost-justifiable capacity always exists to process the agreed workloads and to provide the required performance quality and quantity prescribed in service level agreements. The capacity plan should cover multiple scenarios.

3.8 Resources Availability

CONTROL OBJECTIVE

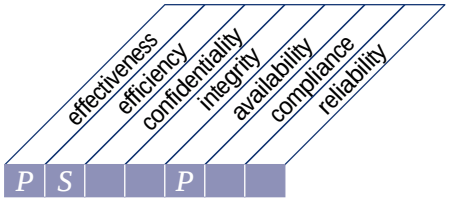
When identified as availability requirements, management should prevent resources from being unavailable by implementing fault tolerance mechanisms, prioritising tasks and equitable resource allocation mechanisms.

3.9 Resources Schedule

CONTROL OBJECTIVE

Management should ensure the timely acquisition of required capacity, taking into account aspects such as resilience, contingency, workloads and storage plans.

HIGH-LEVEL CONTROL OBJECTIVE



Control over the IT process of

ensuring continuous service

that satisfies the business requirement

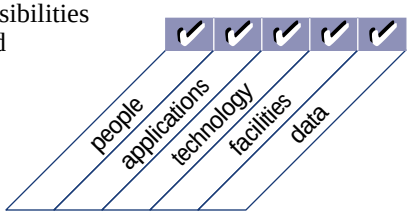
to make sure IT services are available as required and to ensure a minimum business impact in the event of a major disruption

is enabled by

having an operational and tested IT continuity plan which is in line with the overall business continuity plan and its related business requirements

and takes into consideration

- criticality classification
- alternative procedures
- back-up and recovery
- systematic and regular testing and training
- monitoring and escalation processes
- internal and external organisational responsibilities
- business continuity activation, fallback and resumption plans
- risk management activities
- assessment of single points of failure
- problem management



DETAILED CONTROL OBJECTIVES

4 ENSURE CONTINUOUS SERVICE

4.1 IT Continuity Framework

CONTROL OBJECTIVE

IT management, in cooperation with business process owners, should establish a continuity framework which defines the roles, responsibilities and the risk-based approach/methodology to be adopted, and the rules and structures to document the continuity plan as well as the approval procedures.

4.2 IT Continuity Plan Strategy and Philosophy

CONTROL OBJECTIVE

Management should ensure that the IT continuity plan is in line with the overall business continuity plan to ensure consistency. Furthermore, the IT continuity plan should take into account the IT long- and short-range plans to ensure consistency.

4.3 IT Continuity Plan Contents

CONTROL OBJECTIVE

IT management should ensure that a written plan is developed containing the following:

- Guidelines on how to use the continuity plan
- Emergency procedures to ensure the safety of all affected staff members
- Response procedures meant to bring the business back to the state it was in before the incident or disaster
- Recovery procedures meant to bring the business back to the state it was in before the incident or disaster
- Procedures to safeguard and reconstruct the home site
- Co-ordination procedures with public authorities
- Communication procedures with stakeholders, employees, key customers, critical suppliers, stockholders and management
- Critical information on continuity teams, affected staff, customers, suppliers, public authorities and media

4.4 Minimising IT Continuity Requirements

CONTROL OBJECTIVE

IT management should establish procedures and guidelines for minimising the continuity requirements with regard to personnel, facilities, hardware, software, equipment, forms, supplies and furniture.

4.5 Maintaining the IT Continuity Plan

CONTROL OBJECTIVE

IT management should provide for change control procedures in order to ensure that the continuity plan is up-to-date and reflects actual business requirements. This requires continuity plan maintenance procedures aligned with change and management and human resources procedures.

4.6 Testing the IT Continuity Plan

CONTROL OBJECTIVE

To have an effective continuity plan, management needs to assess its adequacy on a regular basis or upon major changes to the business or IT infrastructure; this requires careful preparation, documentation, reporting test results and, according to the results, implementing an action plan.

4.7 IT Continuity Plan Training

CONTROL OBJECTIVE

The disaster continuity methodology should ensure that all concerned parties receive regular training sessions regarding the procedures to be followed in case of an incident or disaster.

continued on next page

DETAILED CONTROL OBJECTIVES *continued*

4.8 **IT Continuity Plan Distribution**
CONTROL OBJECTIVE
Given the sensitive nature of information in the continuity plan, the latter should be distributed only to authorised personnel and should be safeguarded against unauthorised disclosure. Consequently, sections of the plan need to be distributed on a need-to-know basis.

4.9 **User Department Alternative Processing Back-up Procedures**
CONTROL OBJECTIVE
The continuity methodology should ensure that the user departments establish alternative processing procedures that may be used until the IT function is able to fully restore its services after a disaster or an event.

4.10 **Critical IT Resources**
CONTROL OBJECTIVE
The continuity plan should identify the critical application programmes, third-party services, operating systems, personnel and supplies, data files and time frames needed for recovery after a disaster occurs. Critical data and operations should be identified, documented, prioritised and approved by the business process owners, in cooperation with IT management.

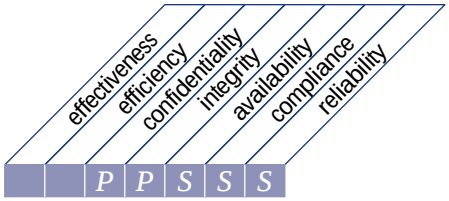
4.11 **Back-up Site and Hardware**
CONTROL OBJECTIVE
Management should ensure that the continuity methodology incorporates an identification of alternatives regarding the back-up site and hardware as well as a final alternative selection. If applicable, a formal contract for these type of services should be concluded.

4.12 **Off-site Back-up Storage**
CONTROL OBJECTIVE
Off-site storage of critical back-up media, documentation and other IT resources should be established to support recovery and business continuity plans. Business process owners and IT function personnel should be involved in determining what back-up resources need to be stored off-site. The off-site storage facility should be environmentally appropriate to the media and other resources stored and should have a level of security commensurate with that needed to protect the back-up resources from unauthorised access, theft or damage. IT management should ensure that off-site arrangements are periodically assessed, at least annually, for content, environmental protection and security.

4.13 **Wrap-up Procedures**
CONTROL OBJECTIVE
On successful resumption of the IT function after a disaster, IT management should establish procedures for assessing the adequacy of the plan and update the plan accordingly.

This page intentionally left blank

HIGH-LEVEL CONTROL OBJECTIVE



Control over the IT process of

ensuring systems security

that satisfies the business requirement

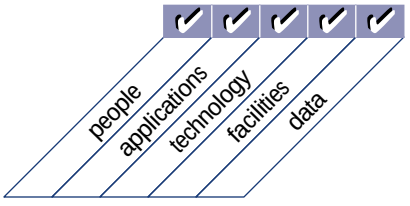
to safeguard information against unauthorised use, disclosure or modification, damage or loss

is enabled by

logical access controls which ensure that access to systems, data and programmes 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



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 of 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 non-disclosure 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 made 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). Also 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 is acted upon in a timely manner.

continued on next page

DETAILED CONTROL OBJECTIVES *continued*

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 need-to-know.

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 keep up-to-date 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.

5.15 **Non-Repudiation**

CONTROL OBJECTIVE

Organisational policy should ensure that, where appropriate, transactions cannot be denied by either party, and controls are implemented to provide non-repudiation 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 is only exchanged 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

All security related hardware and software should at all times be protected against tampering to maintain their integrity and against disclosure of secret keys. 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 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 preventative, 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

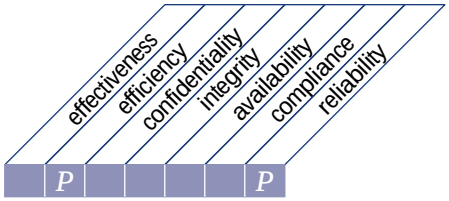
If connection to the Internet or other public networks exists, adequate firewalls should be operative to protect against denial of services and any unauthorised access to the internal resources; should control any application and infrastructure management flows in both directions; and should protect against denial of service attacks.

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.

HIGH-LEVEL CONTROL OBJECTIVE



Control over the IT process of

identifying and allocating costs

that satisfies the business requirement

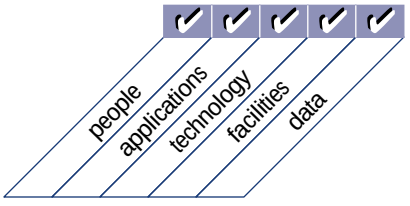
to ensure a correct awareness of the costs attributable to IT services

is enabled by

a cost accounting system which 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 charge-back process
- linkage to service level agreement
- automated reporting
- verification of benefit realisation
- external benchmarking



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

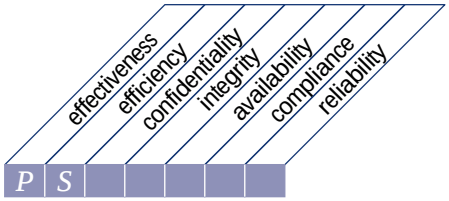
IT management should define and implement costing procedures to provide management information on the costs of delivering information services while ensuring cost effectiveness. Variances between forecasts and actual costs are to be adequately analysed and reported on to facilitate the cost monitoring. 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.

HIGH-LEVEL CONTROL OBJECTIVE



Control over the IT process of

educating and training users

that satisfies the business requirement

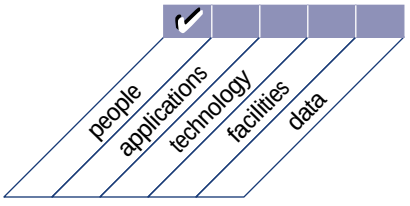
to ensure that users are making effective use of technology and are aware of the risks and responsibilities involved

is enabled by

a comprehensive training and development plan

and takes into consideration

- training curriculum
- skills inventory
- awareness campaigns
- awareness techniques
- use of new training technologies and methods
- personnel productivity
- development of knowledge base



DETAILED CONTROL OBJECTIVES

7 EDUCATE AND TRAIN USERS

7.1 Identification of Training Needs

CONTROL OBJECTIVE

In line with the long-range plan, management should establish and maintain procedures for identifying and documenting the training needs of all personnel using information services. A training curriculum for each group of employees should be established.

7.2 Training Organisation

CONTROL OBJECTIVE

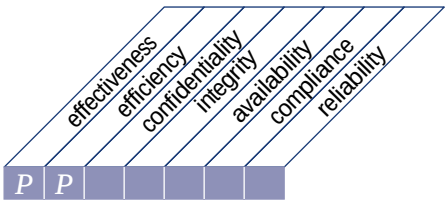
Based on the identified needs, management should define the target groups, identify and appoint trainers, and organise timely training sessions. Training alternatives should also be investigated (internal or external location, in-house trainers or third-party trainers, etc.).

7.3 Security Principles and Awareness Training

CONTROL OBJECTIVE

All personnel must be trained and educated in system security principles, including periodic updates with special focus on security awareness and incident handling. Management should provide an education and training programme that includes: ethical conduct of the IT function, security practices to protect against harm from failures affecting availability, confidentiality, integrity and performance of duties in a secure manner.

HIGH-LEVEL CONTROL OBJECTIVE



Control over the IT process of

assisting and advising customers

that satisfies the business requirement

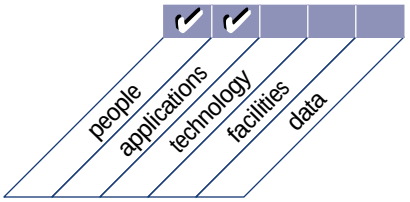
to ensure that any problem experienced by the user is appropriately resolved

is enabled by

a help desk facility which provides first-line support and advice

and takes into consideration

- customer query and problem response
- query monitoring and clearance
- trend analysis and reporting
- development of knowledge base
- root cause analysis
- problem tracking and escalation



DETAILED CONTROL OBJECTIVES

8 ASSIST AND ADVISE CUSTOMERS

8.1 Help Desk

CONTROL OBJECTIVE

User support should be established within a "help desk" function. Individuals responsible for performing this function should closely interact with problem management personnel.

8.2 Registration of Customer Queries

CONTROL OBJECTIVE

Procedures should be in place to ensure that all customer queries are adequately registered by the help desk.

8.3 Customer Query Escalation

CONTROL OBJECTIVE

Help desk procedures should ensure that customer queries which cannot immediately be resolved are appropriately escalated within the IT function.

8.4 Monitoring of Clearance

CONTROL OBJECTIVE

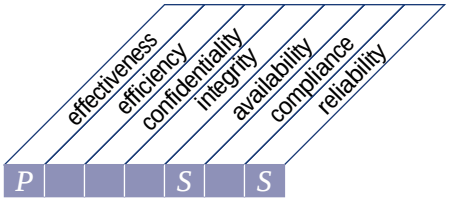
Management should establish procedures for timely monitoring of the clearance of customer queries. Long outstanding queries should be investigated and acted upon.

8.5 Trend Analysis and Reporting

CONTROL OBJECTIVE

Procedures should be in place which assure adequate reporting with regard to customer queries and resolution, response times and trend identification. The reports should be adequately analysed and acted upon.

HIGH-LEVEL CONTROL OBJECTIVE



Control over the IT process of

managing the configuration

that satisfies the business requirement

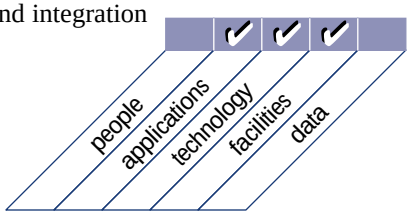
to account for all IT components, prevent unauthorised alterations, verify physical existence and provide a basis for sound change management

is enabled by

controls which identify and record all IT assets and their physical location, and a regular verification programme which confirms their existence

and takes into consideration

- asset tracking
- configuration change management
- checking for unauthorised software
- software storage controls
- software and hardware interrelationships and integration
- use of automated tools



DETAILED CONTROL OBJECTIVES

9 MANAGE THE CONFIGURATION

9.1 Configuration Recording

CONTROL OBJECTIVE

Procedures should be in place to ensure that only authorised and identifiable configuration items are recorded in inventory upon acquisition. These procedures should also provide for the authorised disposal and consequential sale of configuration items. Moreover, procedures should be in place to keep track of changes to the configuration (e.g., new item, status change from development to prototype). Logging and control should be an integrated part of the configuration recording system including reviews of changed records.

9.2 Configuration Baseline

CONTROL OBJECTIVE

IT management should be ensured that a baseline of configuration items is kept as a checkpoint to return to after changes.

9.3 Status Accounting

CONTROL OBJECTIVE

IT management should ensure that the configuration records reflect the actual status of all configuration items including the history of changes.

9.4 Configuration Control

CONTROL OBJECTIVE

Procedures should ensure that the existence and consistency of recording of the IT configuration is periodically checked.

9.5 Unauthorised Software

CONTROL OBJECTIVE

Clear policies restricting the use of personal and unlicensed software should be developed and enforced. The organisation should use virus detection and remedy software. Business and IT management should periodically check the organisation's personal computers for unauthorised software. Compliance with the requirements of software and hardware license agreements should be reviewed on a periodic basis.

9.6 Software Storage

CONTROL OBJECTIVE

A file storage area (library) should be defined for all valid software items in appropriate phases of the system development life cycle. These areas should be separated from each other and from development, testing and production file storage areas.

9.7 Configuration Management Procedures

CONTROL OBJECTIVE

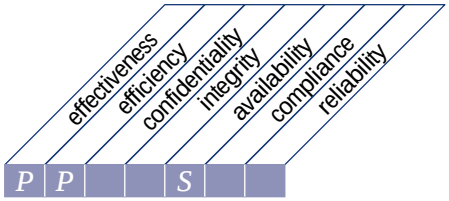
Configuration management procedures should be established to ensure that critical components of the organisation's IT resources have been appropriately identified and are maintained. There should be an integrated process whereby current and future processing demands are measured and provide input to the IT resource acquisitions process.

9.8 Software Accountability

CONTROL OBJECTIVE

Software should be labeled, inventoried and properly licensed. Library management software should be used to produce audit trails of program changes and to maintain program version numbers, creation-date information and copies of previous versions.

HIGH-LEVEL CONTROL OBJECTIVE



Control over the IT process of

managing problems and incidents

that satisfies the business requirement

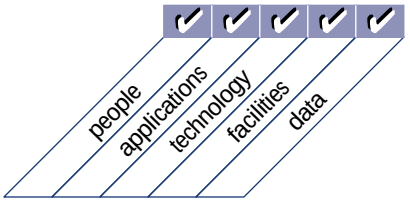
to ensure that problems and incidents are resolved, and the cause investigated to prevent any recurrence

is enabled by

a problem management system which records and progresses all incidents

and takes into consideration

- audit trails of problems and solutions
- timely resolution of reported problems
- escalation procedures
- incident reports
- accessibility of configuration information
- supplier responsibilities
- coordination with change management



DETAILED CONTROL OBJECTIVES

10 MANAGE PROBLEMS AND INCIDENTS

10.1 Problem Management System

CONTROL OBJECTIVE

IT management should define and implement a problem management system to ensure that all operational events which are not part of the standard operation (incidents, problems and errors) are recorded, analysed and resolved in a timely manner. Emergency programme change procedures should be promptly tested, documented, approved and reported. Incident reports should be established in the case of significant problems.

10.2 Problem Escalation

CONTROL OBJECTIVE

IT management should define and implement problem escalation procedures to ensure that identified problems are solved in the most efficient way on a timely basis. These procedures should ensure that these priorities are appropriately set. The procedures should also document the escalation process for the activation of the IT continuity plan.

10.3 Problem Tracking and Audit Trail

CONTROL OBJECTIVE

The problem management system should provide for adequate audit trail facilities which allow tracing from incident to underlying cause (e.g., package release or urgent change implementation) and back. It should closely interwork with change management, availability management and configuration management.

10.4 Emergency and Temporary Access Authorisations

CONTROL OBJECTIVE

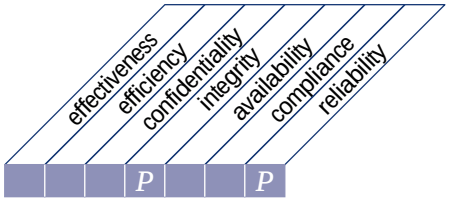
Emergency and temporary access authorisations should be documented on standard forms and maintained on file, approved by appropriate managers, securely communicated to the security function and automatically terminated after a predetermined period.

10.5 Emergency Processing Priorities

CONTROL OBJECTIVE

Emergency processing priorities should be established, documented and approved by appropriate program and IT management.

HIGH-LEVEL CONTROL OBJECTIVE



Control over the IT process of

managing data

that satisfies the business requirement

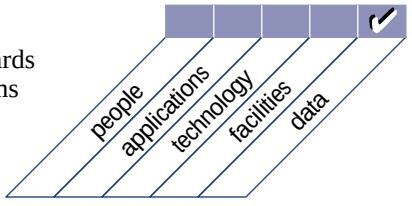
to ensure that data remains complete, accurate and valid during its input, update and storage

is enabled by

an effective combination of application and general controls over the IT operations

and takes into consideration

- form design
- source document controls
- input, processing and output controls
- media identification, movement and library management
- data back-up and recovery
- authentication and integrity
- data ownership
- data administration policies
- data models and data representation standards
- integration and consistency across platforms
- legal and regulatory requirements



DETAILED CONTROL OBJECTIVES

11 MANAGE DATA

11.1 Data Preparation Procedures
CONTROL OBJECTIVE
Management should establish data preparation procedures to be followed by user departments. In this context, input form design should help to assure that errors and omissions are minimised. Error handling procedures during data origination should reasonably ensure that errors and irregularities are detected, reported and corrected.

11.2 Source Document Authorisation Procedures
CONTROL OBJECTIVE
Management should ensure that source documents are properly prepared by authorised personnel who are acting within their authority and that an adequate segregation of duties is in place regarding the origination and approval of source documents.

11.3 Source Document Data Collection
CONTROL OBJECTIVE
The organisation's procedures should ensure that all authorised source documents are complete and accurate, properly accounted for and transmitted in a timely manner for entry.

11.4 Source Document Error Handling
CONTROL OBJECTIVE
Error handling procedures during data origination should reasonably ensure that errors and irregularities are detected, reported and corrected.

11.5 Source Document Retention
CONTROL OBJECTIVE
Procedures should be in place to ensure original source documents are retained or are reproducible by the organisation for an adequate amount of time to facilitate retrieval or reconstruction of data as well as to satisfy legal requirements.

11.6 Data Input Authorisation Procedures
CONTROL OBJECTIVE
The organisation should establish appropriate procedures to ensure that data input is performed only by authorised staff.

11.7 Accuracy, Completeness and Authorisation Checks
CONTROL OBJECTIVE
Transaction data entered for processing (people-generated, system-generated or interfaced inputs) should be subject to a variety of controls to check for accuracy, completeness and validity. Procedures should also be established to assure that input data is validated and edited as close to the point of origination as possible.

11.8 Data Input Error Handling
CONTROL OBJECTIVE
The organisation should establish procedures for the correction and resubmission of data which was erroneously input.

11.9 Data Processing Integrity
CONTROL OBJECTIVE
The organisation should establish procedures for the processing of data that ensure separation of duties is maintained and that work performed is routinely verified. The procedures should ensure adequate update controls such as run-to-run control totals and master file update controls are in place.

11.10 Data Processing Validation and Editing
CONTROL OBJECTIVE
The organisation should establish procedures to ensure that data processing validation, authentication and editing are performed as close to the point of origination as possible. When using Artificial Intelligence systems, these systems should be placed in an interactive control framework with human operators to ensure that vital decisions are approved.

continued on next page

DETAILED CONTROL OBJECTIVES *continued*

11.11 **Data Processing Error Handling**
CONTROL OBJECTIVE
The organisation should establish data processing error handling procedures that enable erroneous transactions to be identified without being processed and without undue disruption of the processing of other valid transactions.

11.12 **Output Handling and Retention**
CONTROL OBJECTIVE
The organisation should establish procedures for the handling and retention of output from its IT application programs. In case negotiable instruments (e.g., value cards) are the output recipients, special care should be taken to prevent misuse.

11.13 **Output Distribution**
CONTROL OBJECTIVE
The organisation should establish and communicate written procedures for the distribution of IT output.

11.14 **Output Balancing and Reconciliation**
CONTROL OBJECTIVE
The organisation should establish procedures for assuring that output routinely is balanced to the relevant control totals. Audit trails should be provided to facilitate the tracing of transaction processing and the reconciliation of disrupted data.

11.15 **Output Review and Error Handling**
CONTROL OBJECTIVE
The organisation's management should establish procedures for assuring that the accuracy of output reports is reviewed by the provider and the relevant users. Procedures should also be in place for controlling errors contained in the output.

11.16 **Security Provision for Output Reports**
CONTROL OBJECTIVE
The organisation should establish procedures for assuring that the security of output reports is maintained for those awaiting distribution, as well as those already distributed to users.

11.17 **Protection of Sensitive Information During Transmission and Transport**
CONTROL OBJECTIVE
Management should ensure that adequate protection of sensitive information is provided during transmission and transport against unauthorised access, modification and misaddressing.

11.18 **Protection of Disposed Sensitive Information**
CONTROL OBJECTIVE
Management should define and implement procedures to prevent access to sensitive information and software from computers, disks and other equipment or media when they are disposed of or transferred to another use. Such procedures should guarantee that data marked as deleted or to be disposed cannot be retrieved by any internal or third party.

11.19 **Storage Management**
CONTROL OBJECTIVE
Procedures should be developed for data storage which consider retrieval requirements, and cost effectiveness and security policy.

11.20 **Retention Periods and Storage Terms**
CONTROL OBJECTIVE
Retention periods and storage terms should be defined for documents, data, programmes and reports and messages (incoming and outgoing) as well as the data (keys, certificates) used for their encryption and authentication.

11.21 **Media Library Management System**
CONTROL OBJECTIVE
The IT function should establish procedures to assure that contents of its media library containing data are inventoried systematically, that any discrepancies disclosed by a physical inventory are remedied in a timely fashion and that measures are taken to maintain the integrity of magnetic media stored in the library.

11.22 **Media Library Management Responsibilities**
CONTROL OBJECTIVE
Housekeeping procedures designed to protect media library contents should be established by IT management. Standards should be defined for the external identification of magnetic media and the control of their physical movement and storage to support accountability. Responsibilities for media (magnetic tape, cartridge, disks and diskettes) library management should be assigned to specific members of the IT function.

11.23 **Back-up and Restoration**
CONTROL OBJECTIVE
Management should implement a proper strategy for back-up and restoration to ensure that it includes a review of business requirements, as well as the development, implementation, testing and documentation of the recovery plan. Procedures should be set up to ensure that back-ups are satisfying the above-mentioned requirements.

11.24 **Back-up Jobs**
CONTROL OBJECTIVE
Procedures should be in place to ensure back-ups are taken in accordance with the defined back-up strategy and the usability of back-ups is regularly verified.

11.25 **Back-up Storage**
CONTROL OBJECTIVE
Back-up procedures for IT-related media should include the proper storage of the data files, software and related documentation, both on-site and off-site. Back-ups should be stored securely and the storage sites periodically reviewed regarding physical access security and security of data files and other items.

11.26 **Archiving**
CONTROL OBJECTIVE
Management should implement a policy and procedures for ensuring that archival meets legal and business requirements, and is properly safeguarded and accounted for.

11.27 **Protection of Sensitive Messages**
CONTROL OBJECTIVE
Regarding data transmission over the Internet or any other public network, management should define and implement procedures and protocols to be used to ensure integrity, confidentiality and non-repudiation of sensitive messages.

11.28 **Authentication and Integrity**
CONTROL OBJECTIVE
The authentication and integrity of information originated outside the organisation, whether received by telephone, voicemail, paper document, fax or e-mail, should be appropriately checked before potentially critical action is taken.

continued on next page

DETAILED CONTROL OBJECTIVES *continued*

11.29 **Electronic Transaction Integrity**

CONTROL OBJECTIVE

Taking into consideration that the traditional boundaries of time and geography are less reliant, management should define and implement appropriate procedures and practices for sensitive and critical electronic transactions ensuring integrity and authenticity of:

- atomicity (indivisible unit of work, all of its actions succeed or they all fail)
- consistency (if the transaction cannot achieve a stable end state, it must return the system to its initial state)
- isolation (a transaction's behavior is not affected by other transactions that execute concurrently)
- durability (transaction's effects are permanent after it commits, its changes should survive system failures)

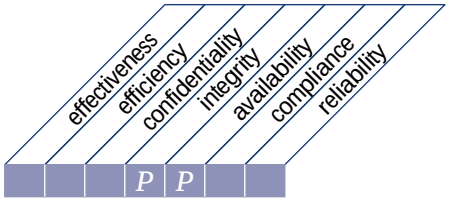
11.30 **Continued Integrity of Stored Data**

CONTROL OBJECTIVE

Management should ensure that the integrity and correctness of the data kept on files and other media (e.g., electronic cards) is checked periodically. Specific attention should be paid to value tokens, reference files and files containing privacy information.

This page intentionally left blank

HIGH-LEVEL CONTROL OBJECTIVE



Control over the IT process of

managing facilities

that satisfies the business requirement

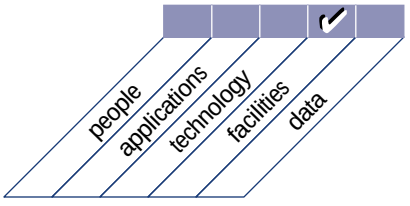
to provide a suitable physical surrounding which protects the IT equipment and people against man-made and natural hazards

is enabled by

the installation of suitable environmental and physical controls which are regularly reviewed for their proper functioning

and takes into consideration

- access to facilities
- site identification
- physical security
- inspection and escalation policies
- business continuity planning and crisis management
- personnel health and safety
- preventive maintenance policies
- environmental threat protection
- automated monitoring



DETAILED CONTROL OBJECTIVES

12 MANAGE FACILITIES

12.1 Physical Security

CONTROL OBJECTIVE

Appropriate physical security and access control measures should be established for IT facilities, including off-site use of information devices in conformance with the general security policy. Physical security and access controls should address not only the area containing system hardware, but also locations of wiring used to connect elements of the system, supporting services (such as electric power), backup media and any other elements required for the system's operation. Access should be restricted to individuals who have been authorised to gain such access. Where IT resources are located in public areas, they should be appropriately protected to prevent or deter loss or damage from theft or vandalism.

12.2 Low Profile of the IT Site

CONTROL OBJECTIVE

IT management should ensure a low profile is kept and the physical identification of the site of the IT operations is limited.

12.3 Visitor Escort

CONTROL OBJECTIVE

Appropriate procedures are to be in place ensuring that individuals who are not members of the IT function's operations group are escorted by a member of that group when they must enter the computer facilities. A visitor's log should be kept and reviewed regularly.

12.4 Personnel Health and Safety

CONTROL OBJECTIVE

Health and safety practices should be put in place and maintained in conformance with applicable international, national, regional, state and local laws and regulations.

12.5 Protection Against Environmental Factors

CONTROL OBJECTIVE

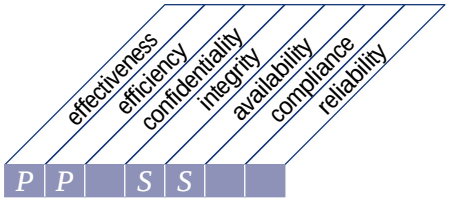
IT management should assure that sufficient measures are put in place and maintained for protection against environmental factors (e.g., fire, dust, power, excessive heat and humidity). Specialised equipment and devices to monitor and control the environment should be installed.

12.6 Uninterruptible Power Supply

CONTROL OBJECTIVE

Management should assess regularly the need for uninterruptable power supply batteries and generators for critical IT applications to secure against power failures and fluctuations. When justified, the most appropriate equipment should be installed.

HIGH-LEVEL CONTROL OBJECTIVE



Control over the IT process of

managing operations

that satisfies the business requirement

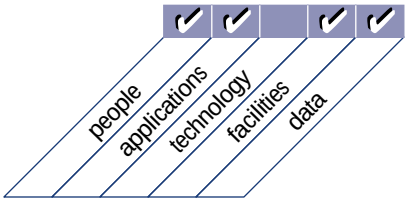
to ensure that important IT support functions are performed regularly and in an orderly fashion

is enabled by

a schedule of support activities which is recorded and cleared for the accomplishment of all activities

and takes into consideration

- operations procedure manual
- start-up process documentation
- network services management
- workload and personnel scheduling
- shift hand-over process
- system event logging
- coordination with change, availability and business continuity management
- preventive maintenance
- service level agreements
- automated operations
- incident logging, tracking and escalation



DETAILED CONTROL OBJECTIVES

13 MANAGE OPERATIONS

13.1 Processing Operations Procedures and Instructions Manual

CONTROL OBJECTIVE

IT management should establish and document standard procedures for IT operations (including network operations). All IT solutions and platforms in place should be operated using these procedures, which should be reviewed periodically to ensure effectiveness and adherence.

13.2 Start-up Process and Other Operations Documentation

CONTROL OBJECTIVE

IT management should ensure that the operations staff is adequately familiar and confident with the start-up process and other operations tasks by having them documented, periodically tested and adjusted when required.

13.3 Job Scheduling

CONTROL OBJECTIVE

IT management should ensure that the continuous scheduling of jobs, processes and tasks is organised into the most efficient sequence, maximising throughput and utilisation, to meet the objectives set in service level agreements. The initial schedules as well as changes to these schedules should be appropriately authorised.

13.4 Departures from Standard Job Schedules

CONTROL OBJECTIVE

Procedures should be in place to identify, investigate and approve departures from standard job schedules.

13.5 Processing Continuity

CONTROL OBJECTIVE

Procedures should require processing continuity during operator shift changes by providing for formal handover of activity, status updates and reports on current responsibilities.

13.6 Operations Logs

CONTROL OBJECTIVE

Management controls should guarantee that sufficient chronological information is being stored in operations logs to enable the reconstruction, review and examination of the time sequences of processing and the other activities surrounding or supporting processing.

13.7 Safeguard Special Forms and Output Devices

CONTROL OBJECTIVE

Management should establish appropriate physical safeguards over special forms, such as negotiable instruments, and over sensitive output devices, such as signature cartridges, taking into consideration proper accounting of IT resources, forms or items requiring additional protection and inventory management.

13.8 Remote Operations

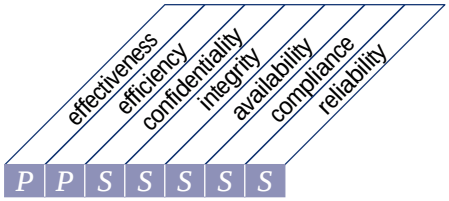
CONTROL OBJECTIVE

For remote operations, specific procedures should ensure that the connection and disconnection of the links to the remote site(s) are defined and implemented.

This page intentionally left blank

MONITORING

HIGH-LEVEL CONTROL OBJECTIVE



Control over the IT process of

monitoring the processes

that satisfies the business requirement

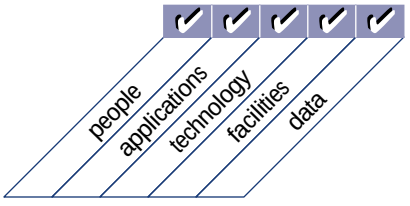
to ensure the achievement of the performance objectives set for the IT processes

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



DETAILED CONTROL OBJECTIVES

1 MONITOR THE PROCESSES

1.1 Collecting Monitoring Data

CONTROL OBJECTIVE

For the IT and internal control processes, management should ensure relevant performance indicators (e.g., benchmarks) from both internal and external sources are being defined, and that data is being 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 be compared with target levels. Assessments of the IT function should be performed on a continuous basis.

1.3 Assessing Customer Satisfaction

CONTROL OBJECTIVE

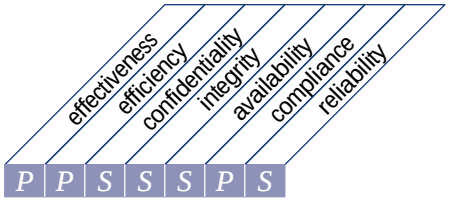
At regular intervals management should measure customer satisfaction regarding the services delivered by the IT function to identify shortfalls in service levels and establish improvement objectives.

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.

HIGH-LEVEL CONTROL OBJECTIVE



Control over the IT process of

assessing internal control adequacy

that satisfies the business requirement

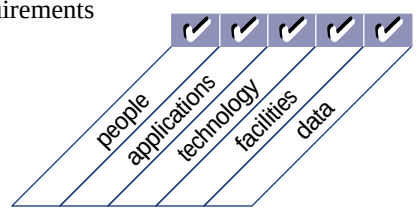
to ensure the achievement of the internal control objectives set for the IT processes

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



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 also 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 are 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

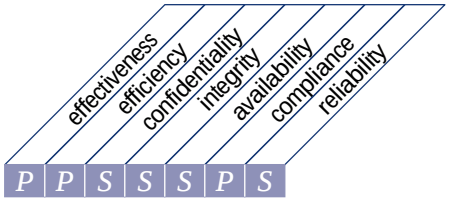
Management should report information on internal control levels and exceptions to the affected parties to ensure the continued effectiveness of its internal control system. Actions should be taken to identify what information is needed at a particular level of decision making.

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.

HIGH-LEVEL CONTROL OBJECTIVE



Control over the IT process of

obtaining independent assurance

that satisfies the business requirement

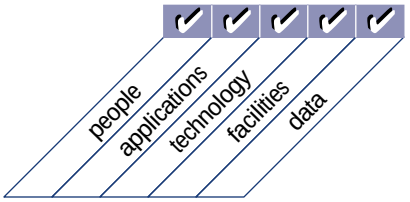
to increase confidence and trust among the organisation, customers, and third-party providers

is enabled by

independent assurance reviews carried out at regular intervals

and takes into consideration

- independent certifications and accreditation
- independent effectiveness evaluations
- independent assurance of compliance with laws and regulatory requirements
- independent assurance of compliance with contractual commitments
- third-party service provider reviews and benchmarking
- performance of assurance reviews by qualified personnel
- proactive audit involvement



DETAILED CONTROL OBJECTIVES

3 OBTAIN INDEPENDENT ASSURANCE

3.1 Independent Security and Internal Control Certification/Accreditation of IT Services

CONTROL OBJECTIVE

Management should obtain independent certification/accreditation of security and internal controls prior to implementing critical new IT services and re-certification/ re-accreditation of these services on a routine cycle after implementation.

3.2 Independent Security and Internal Control Certification/Accreditation of Third-Party Service Providers

CONTROL OBJECTIVE

Management should obtain independent certification/accreditation of security and internal controls prior to using IT service providers and re-certification/re-accreditation on a routine cycle.

3.3 Independent Effectiveness Evaluation of IT Services

CONTROL OBJECTIVE

Management should obtain independent evaluation of the effectiveness of IT services on a routine cycle.

3.4 Independent Effectiveness Evaluation of Third-Party Service Providers

CONTROL OBJECTIVE

Management should obtain independent evaluation of the effectiveness of IT service providers on a routine cycle.

3.5 Independent Assurance of Compliance with Laws and Regulatory Requirements and Contractual Commitments

CONTROL OBJECTIVE

Management should obtain independent assurance of the IT function's compliance with legal and regulatory requirements, and contractual commitments on a routine cycle.

3.6 Independent Assurance of Compliance with Laws and Regulatory Requirements and Contractual Commitments by Third-Party Service Providers

CONTROL OBJECTIVE

Management should obtain independent assurance of third-party service providers' compliance with legal and regulatory requirements and contractual commitments on a routine cycle.

3.7 Competence of Independent Assurance Function

CONTROL OBJECTIVE

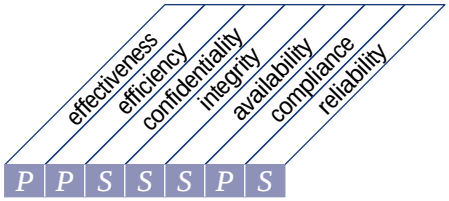
Management should ensure that the independent assurance function possesses the technical competence, and skills and knowledge necessary to perform such reviews in an effective, efficient and economical manner.

3.8 Proactive Audit Involvement

CONTROL OBJECTIVE

IT management should seek audit involvement in a proactive manner before finalising IT service solutions.

HIGH-LEVEL CONTROL OBJECTIVE



Control over the IT process of

providing for independent audit

that satisfies the business requirement

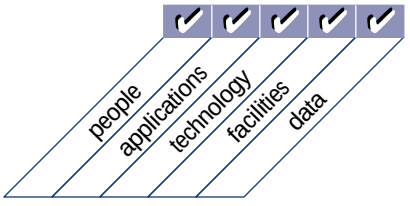
to increase confidence levels and benefit from best practice advice

is enabled by

independent audits carried out at regular intervals

and takes into consideration

- audit independence
- proactive audit involvement
- performance of audits by qualified personnel
- clearance of findings and recommendations
- follow-up activities
- impact assessments of audit recommendations (costs, benefits and risks)



DETAILED CONTROL OBJECTIVES

4 PROVIDE FOR INDEPENDENT AUDIT

4.1 Audit Charter

CONTROL OBJECTIVE

A charter for the audit function should be established by the organisation's senior management. This document should outline the responsibility, authority and accountability of the audit function. The charter should be reviewed periodically to assure that the independence, authority and accountability of the audit function are maintained.

4.2 Independence

CONTROL OBJECTIVE

The auditor should be independent from the auditee in attitude and appearance (actual and perceived). Auditors should not be affiliated with the section or department being audited, and, to the extent possible, should also be independent of the subject organisation itself. Thus, the audit function is to be sufficiently independent of the area being audited to permit objective completion of the audit.

4.3 Professional Ethics and Standards

CONTROL OBJECTIVE

The audit function should ensure adherence to applicable codes of professional ethics (e.g., Code of Professional Ethics of the Information Systems Audit and Control Association) and auditing standards (e.g., Standards for Information Systems Auditing of the Information Systems Audit and Control Association) in all that they do. Due professional care should be exercised in all aspects of the audit work, including the observance of applicable audit and IT standards.

4.4 Competence

CONTROL OBJECTIVE

Management should ensure that the auditors responsible for the review of the organisation's IT activities are technically competent and collectively possess the skills and knowledge (i.e., CISA domains) necessary to perform such reviews in an effective, efficient and economical manner. Management should ensure that audit staff assigned to information systems auditing tasks maintain their technical competence through appropriate continuing professional education.

4.5 Planning

CONTROL OBJECTIVE

Senior management should establish a plan to ensure that regular and independent audits are obtained regarding the effectiveness, efficiency and economy of security and internal control procedures, and management's ability to control IT function activities. Senior management should determine priorities with regard to obtaining independent audits within this plan. Auditors should plan the information systems audit work to address the audit objectives and to comply with applicable professional auditing standards.

4.6 Performance of Audit Work

CONTROL OBJECTIVE

Audits should be appropriately supervised to provide assurances that audit objectives are achieved and applicable professional auditing standards are met. Auditors should ensure that they obtain sufficient, reliable, relevant and useful evidence to achieve the audit objectives effectively. The audit findings and conclusions are to be supported by appropriate analysis and interpretation of this evidence.

continued on next page

DETAILED CONTROL OBJECTIVES *continued*

4.7 **Reporting**

CONTROL OBJECTIVE

The organisation's audit function should provide a report, in an appropriate form, to intended recipients upon the completion of audit work. The audit report should state the scope and objectives of the audit, the period of coverage, and the nature and extent of the audit work performed. The report should identify the organisation, the intended recipients and any restrictions on circulation. The audit report should also state the findings, conclusions and recommendations concerning the audit work performed, and any reservations or qualifications that the auditor has with respect to the audit.

4.8 **Follow-up Activities**

CONTROL OBJECTIVE

Resolution of audit comments rests with management. Auditors should request and evaluate appropriate information on previous findings, conclusions and recommendations to determine whether appropriate actions have been implemented in a timely manner.

APPENDICES

This page intentionally left blank

IT GOVERNANCE MANAGEMENT GUIDELINE

The following Management Guideline and Maturity Model identify the Critical Success Factors (CSFs), Key Goal Indicators (KGIs), Key Performance Indicators (KPIs) and Maturity Model for **IT governance.** First, IT governance is defined, articulating the business need. Next, the information criteria related to IT governance are identified. The business need is measured by the KGIs and enabled by a control statement, leveraged by all the IT resources. The achievement of the enabling control statement is measured by the KPIs, which consider the CSFs. The Maturity Model is used to evaluate an organisation's level of achievement of IT governance—from Non-existent (the lowest level) to Initial/Ad Hoc, to Repeatable but Intuitive, to Defined Process, to Managed and Measurable, to Optimised (the highest level). To achieve the Optimised maturity level for IT governance, an organisation must be at least at the Optimised level for the Monitoring domain and at least at the Managed and Measurable level for all other domains.

(See the COBIT *Management Guidelines* for a thorough discussion of the use of these tools.)

IT GOVERNANCE MANAGEMENT GUIDELINE

Governance over information technology and its processes with the business goal of adding value, while balancing risk versus return

ensures delivery of information to the business that addresses the required Information Criteria and is measured by Key Goal Indicators

is enabled by *creating and maintaining a system of process and control excellence appropriate for the business that directs and monitors the business value delivery of IT*

considers Critical Success Factors that leverage all IT Resources and is measured by Key Performance Indicators

Information Criteria
effectiveness
efficiency
confidentiality
integrity
availability
compliance
reliability

IT Resources
people
applications
technology
facilities
data

Critical Success Factors

- IT governance activities are integrated into the enterprise governance process and leadership behaviours
- IT governance focuses on the enterprise goals, strategic initiatives, the use of technology to enhance the business and on the availability of sufficient resources and capabilities to keep up with the business demands
- IT governance activities are defined with a clear purpose, documented and implemented, based on enterprise needs and with unambiguous accountabilities
- Management practices are implemented to increase efficient and optimal use of resources and increase the effectiveness of IT processes
- Organisational practices are established to enable: sound oversight; a control environment/culture; risk assessment as standard practice; degree of adherence to established standards; monitoring and follow up of control deficiencies and risks
- Control practices are defined to avoid breakdowns in internal control and oversight
- There is integration and smooth interoperability of the more complex IT processes such as problem, change and configuration management
- An audit committee is established to appoint and oversee an independent auditor, focusing on IT when driving audit plans, and review the results of audits and third-party reviews.

Key Goal Indicators

- Enhanced performance and cost management
- Improved return on major IT investments
- Improved time to market
- Increased quality, innovation and risk management
- Appropriately integrated and standardised business processes
- Reaching new and satisfying existing customers
- Availability of appropriate bandwidth, computing power and IT delivery mechanisms
- Meeting requirements and expectations of the customer of the process on budget and on time
- Adherence to laws, regulations, industry standards and contractual commitments
- Transparency on risk taking and adherence to the agreed organisational risk profile
- Benchmarking comparisons of IT governance maturity
- Creation of new service delivery channels

Key Performance Indicators

- Improved cost-efficiency of IT processes (costs vs. deliverables)
- Increased number of IT action plans for process improvement initiatives
- Increased utilisation of IT infrastructure
- Increased satisfaction of stakeholders (survey and number of complaints)
- Improved staff productivity (number of deliverables) and morale (survey)
- Increased availability of knowledge and information for managing the enterprise
- Increased linkage between IT and enterprise governance
- Improved performance as measured by IT balanced scorecards

IT Governance Maturity Model

Governance over information technology and its processes with the business goal of adding value, while balancing risk versus return

0 Non-existent There is a complete lack of any recognisable IT governance process. The organisation has not even recognised that there is an issue to be addressed and hence there is no communication about the issue.

1 Initial / Ad Hoc There is evidence that the organisation has recognised that IT governance issues exist and need to be addressed. There are, however, no standardised processes, but instead there are ad hoc approaches applied on an individual or case-by-case basis. Management's approach is chaotic and there is only sporadic, non-consistent communication on issues and approaches to address them. There may be some acknowledgement of capturing the value of IT in outcome-oriented performance of related enterprise processes. There is no standard assessment process. IT monitoring is only implemented reactively to an incident that has caused some loss or embarrassment to the organisation.

2 Repeatable but Intuitive There is global awareness of IT governance issues. IT governance activities and performance indicators are under development, which include IT planning, delivery and monitoring processes. As part of this effort, IT governance activities are formally established into the organisation's change management process, with active senior management involvement and oversight. Selected IT processes are identified for improving and/or controlling core enterprise processes and are effectively planned and monitored as investments, and are derived within the context of a defined IT architectural framework. Management has identified basic IT governance measurements and assessment methods and techniques, however, the process has not been adopted across the organisation. There is no formal training and communication on governance standards and responsibilities are left to the individual. Individuals drive the governance processes within various IT projects and processes. Limited governance tools are chosen and implemented for gathering governance metrics, but may not be used to their full capacity due to a lack of expertise in their functionality.

3 Defined Process The need to act with respect to IT governance is understood and accepted. A baseline set of IT governance indicators is developed, where linkages between outcome measures and performance drivers are defined, documented and integrated into strategic and operational planning and monitoring processes. Procedures have been standardised, documented and implemented. Management has communicated standardised procedures and informal training is established. Performance indicators over all IT governance activities are being recorded and tracked, leading to enterprise-wide improvements. Although measurable, procedures are not sophisticated, but are the formalisation of existing practices. Tools are standardised, using currently available techniques. IT Balanced Business Scorecard ideas are being adopted by the organization. It is, however, left to the individual to get training, to follow the standards and to apply them. Root cause analysis is only occasionally applied. Most processes are monitored against some (baseline) metrics, but any deviation, while mostly being acted upon by individual initiative, would unlikely be detected by management. Nevertheless, overall accountability of key process performance is clear and management is rewarded based on key performance measures.

4 Managed and Measurable There is full understanding of IT governance issues at all levels, supported by formal training. There is a clear understanding of who the customer is and responsibilities are defined and monitored through service level agreements. Responsibilities are clear and process ownership is established. IT processes are aligned with the business and with the IT strategy. Improvement in IT processes is based primarily upon a quantitative understanding and it is possible to monitor and measure compliance with procedures and process metrics. All process stakeholders are aware of risks, the importance of IT and the opportunities it can offer. Management has defined tolerances under which processes must operate. Action is taken in many, but not all cases where processes appear not to be working effectively or

efficiently. Processes are occasionally improved and best internal practices are enforced. Root cause analysis is being standardised. Continuous improvement is beginning to be addressed. There is limited, primarily tactical, use of technology, based on mature techniques and enforced standard tools. There is involvement of all required internal domain experts. IT governance evolves into an enterprise-wide process. IT governance activities are becoming integrated with the enterprise governance process.

5 Optimised There is advanced and forward-looking understanding of IT governance issues and solutions. Training and communication is supported by leading-edge concepts and techniques. Processes have been refined to a level of external best practice, based on results of continuous improvement and maturity modeling with other organisations. The implementation of these policies has led to an organisation, people and processes that are quick to adapt and fully support IT governance requirements. All problems and deviations are root cause analysed and efficient action is expediently identified and initiated. IT is used in an extensive, integrated and optimised manner to automate the workflow and provide tools to improve quality and effectiveness. The risks and returns of the IT processes are defined, balanced and communicated across the enterprise. External experts are leveraged and benchmarks are used for guidance. Monitoring, self-assessment and communication about governance expectations are pervasive within the organisation and there is optimal use of technology to support measurement, analysis, communication and training. Enterprise governance and IT governance are strategically linked, leveraging technology and human and financial resources to increase the competitive advantage of the enterprise.

COBIT PROJECT DESCRIPTION

The COBIT project continues to be supervised by a Project Steering Committee formed by international representatives from industry, academia, government and the security and control profession. The Project Steering Committee has been instrumental in the development of the COBIT *Framework* and in the application of the research results. International working groups were established for the purpose of quality assurance and expert review of the project's interim research and development deliverables. Overall project guidance is provided by the IT Governance Institute.

RESEARCH AND APPROACH FOR EARLIER DEVELOPMENT

Starting with the COBIT *Framework* defined in the 1st edition, the application of international standards and guidelines and research into best practices have led to the development of the control objectives. Audit guidelines were next developed to assess whether these control objectives are appropriately implemented.

Research for the 1st and 2nd editions included the collection and analysis of identified international sources and was carried out by teams in Europe (Free University of Amsterdam), the US (California Polytechnic University) and Australia (University of New South Wales). The researchers were charged with the compilation, review, assessment and appropriate incorporation of international technical standards, codes of conduct, quality standards, professional standards in auditing and industry practices and requirements, as they relate to the *Framework* and to individual control objectives. After collection and analysis, the researchers were challenged to examine each domain and process in depth and suggest new or modified control objectives applicable to that particular IT process. Consolidation of the results was performed by the COBIT Steering Committee and the Director of Research of ISACF.

RESEARCH AND APPROACH FOR THE 3RD EDITION

The COBIT 3rd Edition project consisted of developing the *Management Guidelines* and updating COBIT 2nd Edition based on new and revised international references.

Furthermore, the COBIT *Framework* was revised and enhanced to support increased management control, to introduce performance management and to further develop IT governance. In order to provide management with an application of the *Framework* so that it can assess and make choices for control implementation and improvements over its information and related technology, as well as measure performance, the *Management Guidelines* include Maturity Models, Critical Success Factors, Key Goal Indicators and Key Performance Indicators related to the *Control Objectives*.

Management Guidelines was developed by using a worldwide panel of 40 experts from industry, academia, government and the IT security and control profession. These experts participated in a residential workshop guided by professional facilitators and using development guidelines defined by the COBIT Steering Committee. The workshop was strongly supported by the Gartner Group and PricewaterhouseCoopers, who not only provided thought leadership but also sent several of their experts on control, performance management and information security. The results of the workshop were draft Maturity Models, Critical Success Factors, Key Goal Indicators and Key Performance Indicators for each of COBIT's 34 high-level control objectives. Quality assurance of the initial deliverables was conducted by the COBIT Steering Committee and the results were posted for exposure on the ISACA web site. The *Management Guidelines* document was finally prepared to offer a new management-oriented set of tools, while providing integration and consistency with the COBIT *Framework*.

The update to the *Control Objectives*, based on new and revised international references, was conducted by members of ISACA chapters, under the guidance of COBIT Steering Committee members. The intention was not to perform a global analysis of all material or a redevelopment of the *Control Objectives*, but to provide an incremental update process.

The results of the development of the *Management Guidelines* were then used to revise the COBIT *Framework*, especially the considerations, goals and enabler statements of the high-level control objectives.

COBIT PRIMARY REFERENCE MATERIAL

COSO: Committee of Sponsoring Organisations of the Treadway Commission. *Internal Control — Integrated Framework.* 2 Vols. American Institute of Certified Accountants, New Jersey, 1994.

OECD Guidelines: Organisation for Economic Co-operation and Development. *Guidelines for the Security of Information,* Paris, 1992.

DTI Code of Practice for Information Security Management: Department of Trade and Industry and British Standard Institute. *A Code of Practice for Information Security Management,* London, 1993, 1995.

ISO 9000-3: International Organisation for Standardisation. *Quality Management and Quality Assurance Standards — Part 3: Guidelines for the Application of ISO 9001 to the development, supply and maintenance of software,* Switzerland, 1991.

An Introduction to Computer Security: The NIST Handbook: NIST Special Publication 800-12, National Institute of Standards and Technology, U.S. Department of Commerce, Washington, DC, 1995.

ITIL IT Management Practices: Information Technology Infrastructure Library. Practices and guidelines developed by the Central Computer and Telecommunications Agency (CCTA), London, 1989.

IBAG Framework: Draft Framework from the Infosec Business Advisory Group to SOGIS (Senior Officials Group on Information Security, advising the European Commission), Brussels, 1994.

NSW Premier's Office Statements of Best Practices and Planning Information Management and Techniques: *Statements of Best Practice #1 through #6.* Premier's Department New South Wales, Government of New South Wales, Australia, 1990 through 1994.

Memorandum Dutch Central Bank: *Memorandum on the Reliability and Continuity of Electronic Data Processing in Banking.* De Nederlandsche Bank, Reprint from Quarterly Bulletin #3, Netherlands, 1998.

EDPAF Monograph #7, EDI: An Audit Approach: Jamison, Rodger. *EDI: An Audit Approach,* Monograph Series #7, Information Systems Audit and Control Foundation, Inc., Rolling Meadows, IL, April 1994.

PCIE (President's Council on Integrity and Efficiency) Model Framework: *A Model Framework for Management Over Automated Information Systems.* Prepared jointly by the President's Council on Management Improvement and the President's Council on Integrity and Efficiency, Washington, DC, 1987.

Japan Information Systems Auditing Standards: *Information System Auditing Standard of Japan.* Provided by the Chuo Audit Corporation, Tokyo, August 1994.

CONTROL OBJECTIVES Controls in an Information Systems Environment: Control Guidelines and Audit Procedures: EDP Auditors Foundation (now the Information Systems Audit and Control Foundation), Fourth Edition, Rolling Meadows, IL, 1992.

CISA Job Analysis: Information Systems Audit and Control Association Certification Board. "Certified Information Systems Auditor Job Analysis Study," Rolling Meadows, IL, 1994.

IFAC International Information Technology Guidelines—Managing Security of Information: International Federation of Accountants, New York, 1998.

IFAC International Guidelines on Information Technology Management—Managing Information Technology Planning for Business Impact: International Federation of Accountants, New York, 1999.

Guide for Auditing for Controls and Security, A System Development Life Cycle Approach: *NIST Special Publication 500-153:* National Institute of Standards and Technology, U.S. Department of Commerce, Washington, DC, 1988.

Government Auditing Standards: US General Accounting Office, Washington, DC, 1999.

SPICE: Software Process Improvement and Capability Determination. A standard on software process improvement, British Standards Institution, London, 1995.

Denmark Generally Accepted IT Management Practices: The Institute of State Authorized Accountants, Denmark, 1994.

DRI International, Professional Practices for Business Continuity Planners: Disaster Recovery Institute International. *Guideline for Business Continuity Planners*, St. Louis, MO, 1997.

IIA, SAC Systems Audibility and Control: Institute of Internal Auditors Research Foundation, *Systems Audibility and Control Report*, Altamonte Springs, FL, 1991, 1994.

IIA, Professional Practices Pamphlet 97-1, Electronic Commerce: Institute of Internal Auditors Research Foundation, Altamonte Springs, FL, 1997.

E & Y Technical Reference Series: Ernst & Young, *SAP R/3 Audit Guide*, Cleveland, OH, 1996.

C & L Audit Guide SAP R/3: Coopers & Lybrand, *SAP R/3: Its Use, Control and Audit*, New York, 1997.

ISO IEC JTC1/SC27 Information Technology — Security: International Organisation for Standardisation (ISO) Technical Committee on Information Technology Security, Switzerland, 1998.

ISO IEC JTC1/SC7 Software Engineering: International Organisation for Standardisation (ISO) Technical Committee on Software Process Assessment. *An Assessment Model and Guidance Indicator,* Switzerland, 1992.

ISO TC68/SC2/WG4, Information Security Guidelines for Banking and Related Financial Services: International Organisation for Standardisation (ISO) Technical Committee on Banking and Financial Services, Draft, Switzerland, 1997.

Common Criteria and Methodology for Information Technology Security Evaluation: CSE (Canada), SCSSI (France), BSI (Germany), NLNCSA (Netherlands), CESG (United Kingdom), NIST (USA) and NSA (USA), 1999.

Recommended Practice for EDI: EDIFACT (EDI for Administration Commerce and Trade), Paris, 1987.

TickIT: *Guide to Software Quality Management System Construction and Certification*. British Department of Trade and Industry (DTI), London, 1994

ESF Baseline Control—Communications: European Security Forum, London. *Communications Network Security*, September 1991; *Baseline Controls for Local Area Networks*, September, 1994.

ESF Baseline Control—Microcomputers: European Security Forum, London. *Baseline Controls Microcomputers Attached to Network*, June 1990.

Computerized Information Systems (CIS) Audit Manual: EDP Auditors Foundation (now the Information Systems Audit and Control Foundation), Rolling Meadows, IL, 1992.

Standards for Internal Control in the Federal Government (GAO/AIMD-00-21.3.1): US General Accounting Office, Washington, DC 1999.

Guide for Developing Security Plans for Information Technology: NIST Special Publication 800-18, National Institute for Standards and Technology, US Department of Commerce, Washington, DC, 1998.

Financial Information Systems Control Audit Manual (FISCAM): US General Accounting Office, Washington, DC, 1999.

BS7799-Information Security Management: British Standards Institute, London, 1999.

CICA Information Technology Control Guidelines, 3rd Edition: Canadian Institute of Chartered Accountants, Toronto, 1998.

ISO/IEC TR 1335-n Guidelines for the Management of IT Security (GMITS), Parts 1-5: International Organisation for Standardisation, Switzerland, 1998.

AICPA/CICA SysTrust™ Principles and Criteria for Systems Reliability, Version 1.0: American Institute of Certified Public Accountants, New York, and Canadian Institute of Chartered Accountants, Toronto, 1999.

Glossary of Terms

AICPA	American Institute of Certified Public Accountants
CICA	Canadian Institute of Chartered Accountants
CISA	Certified Information Systems Auditor
CCEB	Common Criteria for Information Technology Security
Control	The policies, procedures, practices and organisational structures designed to provide reasonable assurance that business objectives will be achieved and that undesired events will be prevented or detected and corrected
COSO	Committee of Sponsoring Organisations of the Treadway Commission
DRI	Disaster Recovery Institute International
DTI	Department of Trade and Industry of the United Kingdom
EDIFACT	Electronic Data Interchange for Administration, Commerce and Trade
EDPAF	Electronic Data Processing Auditors Foundation (now ISACF)
ESF	European Security Forum, a cooperation of 70+ primarily European multi-nationals with the goal of researching common security and control issues in IT
GAO	US General Accounting Office
I4	International Information Integrity Institute, similar association as the ESF, with similar goals but primarily US-based and run by Stanford Research Institute
IBAG	Infosec Business Advisory Group, industry representatives who advise the Infosec Committee. This Committee is composed of government officials of the European Community and itself advises the European Commission on IT security matters.
IFAC	International Federation of Accountants
IIA	Institute of Internal Auditors
INFOSEC	Advisory Committee for IT Security Matters to the European Commission
ISACA	Information Systems Audit and Control Association
ISACF	Information Systems Audit and Control Foundation
ISO	International Organisation for Standardisation (with offices in Geneva, Switzerland)
ISO9000	Quality management and quality assurance standards as defined by ISO
IT Control Objective	A statement of the desired result or purpose to be achieved by implementing control procedures in a particular IT activity
ITIL	Information Technology Infrastructure Library
ITSEC	Information Technology Security Evaluation Criteria. The harmonised criteria of France, Germany, the Netherlands and the United Kingdom, since then also supported by the European Commission (see also TCSEC, the US equivalent).
NBS	National Bureau of Standards of the US
NIST (formerly NBS)	National Institute of Standards and Technology, based in Washington, DC
NSW	New South Wales, Australia
OECD	Organisation for Economic Cooperation and Development
OSF	Open Software Foundation
PCIE	President's Council on Integrity and Efficiency
SPICE	Software Process Improvement and Capability Determination—a standard on software process improvement
TCSEC	Trusted Computer System Evaluation Criteria, also known as The Orange Book: security evaluation criteria for computer systems as originally defined by the US Department of Defense. See also ITSEC, the European equivalent.
TickIT	Guide to Software Quality Management System Construction and Certification

INDEX

INDEX

INDEX

INDEX

GOVERNANCE INSTITUTE™

3701 ALGONQUIN ROAD, SUITE 1010
ROLLING MEADOWS, ILLINOIS 60008, USA

TELEPHONE: +1.847.253.1545
FACSIMILE: +1.847.253.1443
E-MAIL: research@isaca.org
WEB SITES: *www.ITgovernance.org*
www.isaca.org

TELL US WHAT YOU THINK ABOUT COBIT

We are interested in knowing your reaction to *COBIT: Control Objectives for Information and related Technology*. Please provide your comments below.

_____

_____

_____

_____

_____

_____

_____

_____

Name _____

Company _____

Address _____

City _____ State/Province _____

Country _____ ZIP/Postal Code _____

FAX Number _____

E-mail Address _____

☐ I am interested in learning more about how COBIT can be used in my organisation. Please ask a representative to contact me.

☐ Please send me more information about:

- ☐ Purchasing other COBIT products
- ☐ COBIT Training Courses (in-house or general session)
- ☐ Certified Information Systems Auditor™ (CISA®) Certification
- ☐ *Information Systems Control Journal*
- ☐ Information Systems Audit and Control Association (ISACA)

Thank you!

All respondents will be acknowledged.