INTERNATIONAL STANDARD

ISO/IEC 20000-2

First edition
2005-12-15

Information technology — Service management —

Part 2: Code of practice

Technologies de l'information — Gestion de services —

Partie 2: Code de bonne pratique

Reference number
ISO/IEC 20000-2:2005(E)

© ISO/IEC 2005

Copyright International Organization for Standardization
Reproduced by IHS under license with ISO
No reproduction or networking permitted without license from IHS

Not for Resale

PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.

© ISO/IEC 2005

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Copyright International Organization for Standardization
Reproduced by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

© ISO/IEC 2005 – All rights reserved

Contents

Page

Foreword v

Introduction vi

1 Scope 1

2 Terms and definitions 2

3 The management system 2
3.1 Management responsibility 2
3.2 Documentation requirements 2
3.3 Competence, awareness and training 3
3.3.1 General 3
3.3.2 Professional development 3
3.3.3 Approaches to be considered 3

4 Planning and implementing service management 4
4.1 Plan service management (Plan) 4
4.1.1 Scope of service management 4
4.1.2 Planning approaches 4
4.1.3 Events to be considered 5
4.1.4 Scope and contents of the plan 5
4.2 Implement service management and provide the services (Do) 6
4.3 Monitoring, measuring and reviewing (Check) 6
4.4 Continual improvement (Act) 6
4.4.1 Policy 6
4.4.2 Planning for service improvements 7

5 Planning and implementing new or changed services 7
5.1 Topics for consideration 7
5.2 Change records 7

6 Service delivery processes 8
6.1 Service level management 8
6.1.1 Service catalogue 8
6.1.2 Service level agreements (SLAs) 8
6.1.3 Service level management (SLM) process 10
6.1.4 Supporting service agreements 10
6.2 Service reporting 10
6.2.1 Policy 10
6.2.2 Purpose and quality checks on service reports 11
6.2.3 Service reports 11
6.3 Service continuity and availability management 11
6.3.1 General 11
6.3.2 Availability monitoring and activities 12
6.3.3 Service continuity strategy 12
6.3.4 Service continuity planning and testing 12
6.4 Budgeting and accounting for IT services 13
6.4.1 General 13
6.4.2 Policy 13
6.4.3 Budgeting 14
6.4.4 Accounting 14
6.5 Capacity management 14
6.6 Information security management 15
6.6.1 General 15
6.6.2 Identifying and classifying information assets 15
6.6.3 Security risk assessment practices 15

© ISO/IEC 2005 – All rights reserved

Copyright International Organization for Standardization
Reproduced by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

6.6.4 Risks to information assets 15
6.6.5 Security and availability of information 16
6.6.6 Controls 16
6.6.7 Documents and records 16

7 Relationship processes 17
7.1 General 17
7.2 Business relationship management 18
7.2.1 Service reviews 18
7.2.2 Service complaints 18
7.2.3 Customer satisfaction measurement 18
7.3 Supplier management 19
7.3.1 Introduction 19
7.3.2 Contract management 19
7.3.3 Service definition 19
7.3.4 Managing multiple suppliers 20
7.3.5 Contractual disputes management 20
7.3.6 Contract end 20

8 Resolution processes 20
8.1 Background 20
8.1.1 Setting priorities 20
8.1.2 Workarounds 21
8.2 Incident management 21
8.2.1 General 21
8.2.2 Major incidents 22
8.3 Problem management 22
8.3.1 Scope of problem management 22
8.3.2 Initiation of problem management 22
8.3.3 Known errors 22
8.3.4 Problem resolution 23
8.3.5 Communication 23
8.3.6 Tracking and escalation 23
8.3.7 Incident and problem record closure 23
8.3.8 Problem reviews 23
8.3.9 Topics for reviews 24
8.3.10 Problem prevention 24

9 Control processes 25
9.1 Configuration management 25
9.1.1 Configuration management planning and implementation 25
9.1.2 Configuration identification 25
9.1.3 Configuration control 26
9.1.4 Configuration status accounting and reporting 27
9.1.5 Configuration verification and audit 27
9.2 Change management 28
9.2.1 Planning and implementation 28
9.2.2 Closing and reviewing the change request 29
9.2.3 Emergency changes 29
9.2.4 Change management reporting, analysis and actions 29

10 Release process 29
10.1 Release management process 29
10.1.1 General 29
10.1.2 Release policy 30
10.1.3 Release and roll-out planning 30
10.1.4 Developing or acquiring software 31
10.1.5 Design, build and configure release 31
10.1.6 Release verification and acceptance 31
10.1.7 Documentation 32
10.1.8 Roll-out, distribution and installation 32
10.1.9 Post release and roll-out 33

Bibliography 34

© ISO/IEC 2005 – All rights reserved
Copyright International Organization for Standardization
Reproduced by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

ISO/IEC 20000-2 was prepared by BSI (as BS 15000-2) and was adopted, under a special “fast-track procedure”, by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, in parallel with its approval by national bodies of ISO and IEC.

ISO/IEC 20000 consists of the following parts, under the general title *Information technology — Service management*:

— *Part 1: Specification*

— *Part 2: Code of practice*

© ISO/IEC 2005 All rights reserved

Copyright International Organization for Standardization
Reproduced by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Introduction

As a code of practice, this part of ISO/IEC 20000 takes the form of guidance and recommendations. It should not be quoted as if it were a specification and particular care should be taken to ensure that claims of compliance are not misleading.

This part of ISO/IEC 20000 should be used in conjunction with ISO/IEC 20000-1, the specification associated with this code of practice.

It is assumed that the execution of the provisions of this part of ISO/IEC 20000 is entrusted to appropriately qualified and competent people. An International Standard does not purport to include all necessary provisions of a contract. Users of International Standards are responsible for their correct application.

Compliance with an International Standard does not of itself confer immunity from legal obligations

This part of ISO/IEC 20000 describes the best practices for service management processes within the scope of ISO/IEC 20000-1.

Service delivery grows in importance, as customers require increasingly advanced facilities (at minimum cost) to meet their business needs. It also recognizes that services and service management are essential to helping organizations generate revenue and be cost-effective.

ISO/IEC 20000-1 is a specification for service management and should be read in conjunction with this part of ISO/IEC 20000.

The ISO/IEC 20000 series enables service providers to understand how to enhance the quality of service delivered to their customers, both internal and external.

With the increasing dependencies in support services and the diverse range of technologies available, service providers can struggle to maintain high levels of customer service. Working reactively, they spend too little time planning, training, reviewing, investigating, and working with customers. The result is a failure to adopt structured, proactive working practices.

Those same service providers are being asked for improved quality, lower costs, greater flexibility, and faster response to customers. Effective service management delivers high levels of customer service and customer satisfaction.

The ISO/IEC 20000 series draws a distinction between the best practices of processes, which are independent of organizational form or size and organizational names and structures. The ISO/IEC 20000 series applies to both large and small service providers, and the requirements for best practice service management processes do not change according to the organizational form which provides the management framework within which processes are followed.

© ISO/IEC 2005 – All rights reserved
Copyright International Organization for Standardization
Reproduced by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Information technology — Service management —

Part 2:
Code of practice

1 Scope

This part of ISO/IEC 20000 represents an industry consensus on quality standards for IT service management processes. These service management processes deliver the best possible service to meet a customer's business needs within agreed resource levels, i.e. service that is professional, cost-effective and with risks which are understood and managed.

The variety of terms used for the same process, and between processes and functional groups (and job titles) can make the subject of service management confusing to the new manager. Failure to understand the terminology can be a barrier to establishing effective processes. Understanding the terminology is a tangible and significant benefit from ISO/IEC 20000. This part of ISO/IEC 20000 recommends that service providers should adopt common terminology and a more consistent approach to service management. It gives a common basis for improvements in services. It also provides a framework for use by suppliers of service management tools.

As a process based standard this code of practice is not intended for product assessment. However, organizations developing service management tools, products and systems may use both the specification and the code of practice to help them develop tools, products and systems that support best practice service management.

This part of ISO/IEC 20000 provides guidance to auditors and offers assistance to service providers planning service improvements or to be audited against ISO/IEC 20000-1.

ISO/IEC 20000-1 specifies a number of related service management processes as shown in Figure 1.

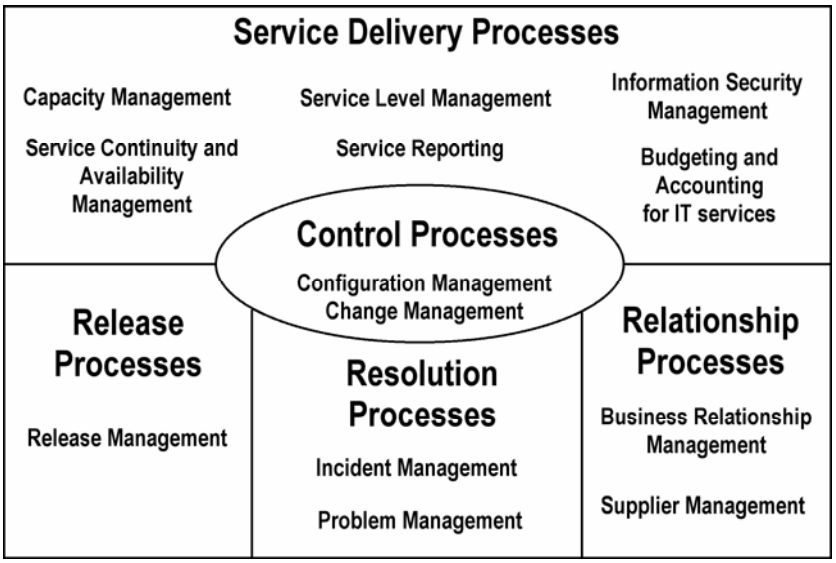

Figure 1 – Service management processes

© ISO/IEC 2005 – All rights reserved

Copyright International Organization for Standardization
Reproduced by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

2 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 20000-1 apply.

3 The management system

Objective: To provide a management system, including policies and a framework to enable the effective management and implementation of all IT services.

3.1 Management responsibility

The role of management in ensuring best practice processes are adopted and sustained is fundamental for any service provider to meet the requirements of ISO/IEC 20000-1.

To ensure commitment an owner at senior level should be identified as being responsible for service management plans. This senior responsible owner should be accountable for the overall delivery of the service management plan.

The senior responsible owner's role should encompass resourcing for any continual or project based service improvement activities.

The senior responsible owner should be supported by a decision-taking group with sufficient authority to define policy and to enforce its decisions.

3.2 Documentation requirements

The senior responsible owner should ensure that evidence is available for an audit of service management policies, plans and procedures, and any activities related to these.

Much of the evidence of service management planning and operations should exist in the form of documents, which may be any type, form or medium suitable for their purpose.

The following documents are normally considered suitable as evidence of service management planning.

a) policies and plans;

b) service documentation;

c) procedures;

d) processes;

e) process control records.

There should be a process for the creation and management of documents to help ensure that the characteristics described are met.

Documentation should be protected from damage due, for example, to poor environmental conditions and computer disasters.

© ISO/IEC 2005 – All rights reserved
Copyright International Organization for Standardization
Reproduced by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

3.3 Competence, awareness and training

3.3.1 General

Personnel performing work within service management should be competent on the basis of appropriate education, training, skills, and experience.

The service provider should:

a) determine the necessary competence for each role in service management;

b) ensure that personnel are aware of the relevance and importance of their activities within the wider business context and how they contribute to the achievement of quality objectives;

c) maintain appropriate records of education, training, skills and experience;

d) provide training or take other action to satisfy these needs;

e) evaluate the effectiveness of the actions taken.

3.3.2 Professional development

The service provider should develop and enhance the professional competence of their workforce. Among the measures taken to achieve this, the service provider should address the following:

a) **recruitment**: with the objective of checking the validity of job applicants' details (including their professional qualifications) and identifying applicants' strengths, weaknesses and potential capabilities, against a job description/profile, service management targets and overall service quality objectives;

b) **planning**: with the objective of staffing of new or expanded services (also contracting services), using new technology, assigning service management staff to development project teams, succession planning and filling other gaps due to anticipated staff turnover;

c) **training and development:** with the objective of identifying training and development requirements as a training and development plan and providing for timely and effective delivery.

Staff should be trained in the relevant aspects of service management (e.g. via training courses, self study, mentoring and on the job training) and their team-working and leadership skills should be developed. A chronological training record should be maintained for each individual, together with descriptions of the training provided.

3.3.3 Approaches to be considered

In order to achieve teams of staff with appropriate levels of competence the service provider should decide on the optimum mix of short term and permanent recruits. The service provider should also decide on the optimum mix of new staff with the skills required and re-training of existing staff.

NOTE The optimum balance of short term and permanent recruits is particularly important when the service provider is planning how to provide a service during and after major changes to the number and skills of the support staff.

Factors that should be considered when establishing the most suitable combination of approaches include:

a) short or long term nature of new or changed competencies;

b) rate of change in the skills and competencies;

c) expected peaks and troughs in the workload and skills mix required, based on service management and service improvement planning;

© ISO/IEC 2005 – All rights reserved

Copyright International Organization for Standardization
Reproduced by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

d) availability of suitably competent staff;

e) staff turnover rates;

f) training plans.

For all staff, the service provider should review each individual's performance at least annually and take appropriate action.

4 Planning and implementing service management

4.1 Plan service management (Plan)

Objective: To plan the implementation and delivery of service management.

4.1.1 Scope of service management

The scope of service management should be defined as part of the service management plan.

For example, it may be defined by

a) organization;

b) location;

c) service.

Management should define the scope as part of their management responsibilities (and as part of the service management plan). The scope should then be checked for suitability under ISO/IEC 20000-1.

NOTE Planning for operational changes is described in **9.2.**

4.1.2 Planning approaches

Multiple service management plans may be used in place of one large plan or programme. Where this is the case the underlying service management processes should be consistent with each other. It should also be possible to demonstrate how each planning requirement is managed by linking it to the corresponding roles, responsibilities and procedures.

Service management planning should form part of the process for translating customers' requirements and senior management intentions into services, and for providing a route map for directing progress.

A service management plan should encompass:

a) implementation of service management (or part of service management);

b) delivery of service management processes;

c) changes to service management processes;

d) improvements to service management processes;

e) new services (to the extent that they affect processes within the agreed scope of service management).

© ISO/IEC 2005 – All rights reserved
Copyright International Organization for Standardization
Reproduced by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

4.1.3 Events to be considered

The service management plan should cater for service management process and service changes triggered by events such as:

a) service improvement;

b) service changes;

c) infrastructure standardization;

d) changes to legislation;

e) regulatory changes, e.g. local tax rate changes;

f) deregulation or regulation of industries;

g) mergers and acquisitions.

4.1.4 Scope and contents of the plan

A service management plan should define:

a) the scope of the service provider's service management;

b) the objectives and requirements that are to be achieved by service management;

c) the resources, facilities and budgets necessary to achieve the defined objectives;

d) the framework of management roles and responsibilities, including the senior responsible owner, process owners and management of suppliers;

e) the interfaces between service management processes and the manner in which the activities and/or processes are to be co-ordinated;

f) the approach to be taken in identifying, assessing and managing issues and risks to the achievement of the defined objectives;

g) a resource schedule expressed in terms of the dates on which funds, skills, and resources should be available;

h) the approach to changing the plan and the service defined by the plan;

i) how the service provider will demonstrate continuing quality control (e.g. interim audits);

j) the processes that are to be executed;

k) tools as appropriate to support the processes.

© ISO/IEC 2005 – All rights reserved

Copyright International Organization for Standardization
Reproduced by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

4.2 Implement service management and provide the services (Do)

Objective: To implement the service management objectives and plan.

Attainment of best practice service management processes capable of meeting the requirements of ISO/IEC 20000 will not be achieved if the original services do not meet the requirements outlined for the implementation in ISO/IEC 20000-1.

Once implemented the service and service management processes should be maintained.

Reviews should take place in accordance with 4.3.

NOTE The person that is appropriate for the planning and initial implementation may not be suitable for the ongoing operation.

4.3 Monitoring, measuring and reviewing (Check)

Objective: To monitor, measure and review that the service management objectives and plan are being achieved.

The service provider should plan and implement the monitoring, measurement, analysis and review of the service, the service management processes and associated systems. Items that should be monitored, measured, and reviewed include:

a) achievement against defined service targets;

b) customer satisfaction;

c) resource utilisation;

d) trends;

e) major non-conformities.

The results of the analysis should provide input to a plan for improving the service.

As well as service management activities on measurement and analysis senior management may need to make use of internal audits and other checks. When deciding the frequency of such internal audits and checks, the degree of risk involved in a process, its frequency of operation and its past history of problems are among the factors that should be taken into account. Internal audits and checks should be planned, carried out competently and recorded.

4.4 Continual improvement (Act)

Objective: To improve the effectiveness and efficiency of service delivery and management.

4.4.1 Policy

Service providers should recognize that there is always the potential to make delivery of services more effective and efficient. There should be a published policy on service quality and improvement.

All those involved in service management and service improvement should be aware of the service quality policy and their personal contribution to the achievement of the objectives laid out within this policy.

In particular all the service provider's staff involved in service management should have a detailed understanding of the implications of this on service management processes.

© ISO/IEC 2005 – All rights reserved
Copyright International Organization for Standardization
Reproduced by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

There should be effective liaison within the service provider's own management structure, customers and the service provider's suppliers on matters affecting service quality and customer requirements.

4.4.2 Planning for service improvements

Service providers should adopt a methodical and coordinated approach to service improvement to meet the requirements of the policy, from their own and from their customer's perspective.

Before implementing a plan for improving the service, service quality and levels should be recorded as a baseline against which the actual improvements can be compared. The actual improvement should be compared to the predicted improvement to assess the effectiveness of the change.

NOTE 1 Service improvement requirements can come from all processes.

Service providers should encourage their staff and customers to suggest ways of improving services.

NOTE 2 This may be done using suggestion schemes, quality circles, user groups and liaison meetings.

Service improvement targets should be measurable, linked to business objectives and documented in a plan.

Service improvement should be actively managed and progress should be monitored against formally agreed objectives.

5 Planning and implementing new or changed services

Objective: To ensure that new services and changes to services will be deliverable and manageable at the agreed cost and service quality.

5.1 Topics for consideration

Planning for new or changed services should include reviewing:

a) budgets;

b) staff resources;

c) existing service levels,

d) SLAs and other targets or service commitments;

e) existing service management processes, procedures and documentation;

f) the scope of service management, including the implementation of service management processes previously excluded from the scope.

5.2 Change records

All service changes should be reflected in Change Management records.

This includes plans for:

a) staff recruitment/retraining;

b) relocation;

c) user training;

© ISO/IEC 2005 – All rights reserved

Copyright International Organization for Standardization
Reproduced by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

d) communications about the changes;

e) changes to the nature of the technology supported;

f) formal closure of services.

6 Service delivery processes

6.1 Service level management

Objective: To define, agree, record, and manage levels of service.

6.1.1 Service catalogue

A service catalogue should define all services. It can be referenced from the SLA and should be used to hold material considered volatile for the SLA itself.

The service catalogue should be maintained and kept up-to-date.

NOTE The service catalogue can include generic information such as:

a) the name of the service;

b) targets, e.g. time to respond or install a printer, time to re-instate a service after a major failure;

c) contact points;

d) service hours and exceptions;

e) security arrangements.

The service catalogue is a key document for setting customer expectation and should be easily accessible and widely available to both customers and support staff.

6.1.2 Service level agreements (SLAs)

A service should be formally documented in a service level agreement (SLA). The SLA should be formally authorized by senior customer and service provider representatives. The SLA should be subject to change management, as is the service that it describes.

The customer's business needs and budget should be the defining force for the content, structure and targets of the SLA. The targets, against which the delivered service should be measured, should be defined from a customer perspective.

The SLAs should include only an appropriate subset of the targets to focus attention on the most important aspects of the service.

NOTE 1 Too many targets can create confusion and lead to excessive overheads.

© ISO/IEC 2005 – All rights reserved
Copyright International Organization for Standardization
Reproduced by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

The minimum content that should be in an SLA or that can be directly referenced from an SLA is:

a) brief service description;

b) validity period and/or SLA change control mechanism;

c) authorization details;

d) brief description of communications, including reporting;

e) contact details of people authorized to act in emergencies, to participate in incidents and problem correction, recovery or workaround;

f) service hours, e.g. 09:00 h to 17:00 h, date exceptions (e.g. weekends, public holidays), critical business periods and out of hours cover;

g) scheduled and agreed interruptions, including notice to be given, number per period;

h) customer responsibilities, e.g. security;

i) service provider liability and obligations e.g. security;

j) impact and priority guidelines;

k) escalation and notification process;

l) complaints procedure;

m) service targets;

n) workload limits (upper and lower), e.g. the ability of the service to support the agreed number of users/volume of work, system throughput;

o) high level financial management details, e.g. charge codes etc;

p) action to be taken in the event of a service interruption;

q) housekeeping procedures;

r) glossary of terms;

s) supporting and related services;

t) any exceptions to the terms given in the SLA.

NOTE 2 Volatile information, or information common to many SLAs (such as contact details) can be referenced from the SLA without impacting the quality of SLM processes as long as the referenced documents are also under the control of the change management process.

NOTE 3 Continuity plan and details of accounting & budgeting are normally referenced from the SLA.

NOTE 4 A glossary of terms is normally held in one place and is common to all documents, including the service catalogue.

--`,,```,,,,````-`-`,,`,,`,`,,`---

© ISO/IEC 2005 – All rights reserved

Copyright International Organization for Standardization
Reproduced by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

6.1.3 Service level management (SLM) process

Major business changes, due, for example, to growth, business reorganizations and mergers, and changing customer requirements, can require service levels to be adjusted, redefined or even temporarily suspended. The SLM process should be flexible to accommodate these changes. The SLM process should ensure that the service provider remains focused on the customer throughout the planning, implementation, and ongoing management of service delivery.

The service provider should be given adequate information to enable them to understand their customer's business drivers and requirements.

The SLM process should manage and coordinate contributors of the service levels, to include:

a) agreement of the service requirements and expected service workload characteristics;

b) agreement of service targets;

c) measurement and reporting of the service levels achieved, workloads and an explanation if the agreed targets are not met (see 6.2);

d) initiation of corrective action;

e) input to a plan for improving the service.

The process should encourage both the service provider and the customer to develop a proactive attitude ensuring that they have joint responsibility for the service.

Customer satisfaction is an important part of service level management but it should be recognized as being a subjective measurement, whereas service targets within an SLA should be objective measurements. The SLM process should work closely with the business relationship and supplier management processes.

6.1.4 Supporting service agreements

The supporting services on which the delivered service depends should be documented and agreed with each supplier. This includes internal groups providing part of the service provider's service.

6.2 Service reporting

Objective: To produce agreed timely, reliable, accurate reports for informed decision making and effective communication.

NOTE The success of all service management processes is dependent on the use of the information provided in service reports.

6.2.1 Policy

The requirements for service reporting should be agreed and recorded for customers and internal management.

Service monitoring and reporting encompasses all measurable aspects of the service, providing both current and historical analysis.

Where there are multiple suppliers, lead suppliers and sub-contracted suppliers the reports should reflect the relationships between suppliers. For example, a lead supplier should report on the whole of the service they provide, including any services by sub-contracted suppliers that they manage as part of the customer's service.

--`,,```,,,,````-`-`,,`,,`,`,,`---

© ISO/IEC 2005 – All rights reserved
Copyright International Organization for Standardization
Reproduced by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

6.2.2 Purpose and quality checks on service reports

Service reports should be timely, clear, reliable, and concise.

They should be appropriate to the recipient's needs and of sufficient accuracy to be used as a decision support tool.

The presentation should aid the understanding of the reports so that they are easy to assimilate, e.g. use of charts.

Several types of report should be produced:

a) reactive reports which show what has happened;

b) proactive reports, which give advance warning of significant events, thereby enabling preventive action to be taken beforehand (for example reports of impending breaches in SLAs);

c) forward scheduled reports showing planned activities.

6.2.3 Service reports

The service provider should produce reports for customers and management covering:

a) performance against service level targets, e.g. outage reports, achievements;

b) non-compliance with standards;

c) workload characteristics and volume information, e.g. incidents, problems, changes and tasks, classification, location, customer, seasonal trends, mix of priorities, numbers of requests for help;

d) performance reporting following major events, e.g. change, and releases;

e) trend information by period (e.g. day, week, month, period);

f) reports that include information from each process, e.g. the number of incidents and the most frequently asked questions, unreliable components of the infrastructure, resource/cost intensive tasks;

g) reports to highlight future and scheduled workloads.

6.3 Service continuity and availability management

Objective: To ensure that agreed service continuity and availability commitments to customers can be met in all circumstances.

NOTE Major service failures or disasters can occur for many reasons including denial of service, attack, major virus outbreak, access to the premises not allowed or a natural disaster.

6.3.1 General

Service continuity and availability requirements should be identified on the basis of the customers' business priorities, service level agreements and assessed risks. The service provider should maintain sufficient service capability together with workable plans designed to ensure that agreed requirements can be met in all circumstances from normal through to a major loss of service. The service provider should plan for known data or user volume increases or decreases, expected peaks and troughs in workload and any other known future changes. Requirements should include access rights and response times as well as end-to-end availability of system components.

--`,,```,,,,````-`-`,,`,,`,`,,`---

© ISO/IEC 2005 – All rights reserved

Copyright International Organization for Standardization
Reproduced by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Service availability and service continuity management should work together with the aim of ensuring that agreed service levels are maintained. These requirements should have a major influence on the actions, efforts and resources allocated to matching the availability of services that support them.

Processes to ensure that required availability is maintained should include those elements of the service delivery that are under the control of the customer or other service providers.

6.3.2 Availability monitoring and activities

Availability management should:

a) monitor and record availability of the service

b) maintain accurate historical data;

c) make comparisons with requirements defined in SLAs to identify non-conformance to the agreed availability targets;

d) document and review non-conformance;

e) predict future availability;

f) where possible, potential issues should be predicted and preventive action taken.

It should ensure availability of all components of the service, with corrective actions recorded and acted upon.

6.3.3 Service continuity strategy

The service provider should develop and maintain a strategy that defines the general approach to be taken to meeting service continuity obligations. This should include risk assessment and take into account agreed service hours and critical business periods. The service provider should agree for each customer group and service:

a) maximum acceptable continuous period of lost service;

b) maximum acceptable periods of degraded service;

c) acceptable degraded service levels during a period of service recovery.

The continuity strategy should be reviewed at agreed intervals, at least annually.

Any changes to the strategy should be formally agreed.

6.3.4 Service continuity planning and testing

The service provider should ensure that:

a) continuity plans take into account dependencies between service and system components;

b) service continuity plans and other documents required to support service continuity are recorded and maintained;

c) responsibility for invoking continuity plans is clearly assigned, and plans clearly allocate responsibility for taking action against each objective;

d) backups of data, documents and software, and any equipment and staff necessary for service restoration are quickly available following a major service failure or disaster;

© ISO/IEC 2005 – All rights reserved
Copyright International Organization for Standardization
Reproduced by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

e) at least one copy of all service continuity documents should be stored and maintained at a secure remote location, together with any equipment that is necessary to enable its use;

f) staff understand their role in invoking and/or executing the plans; and are able to access service continuity documents.

Service continuity plans and related documents (e.g. contracts) should be linked to the change management process and the contract management process.

Service continuity plans and related documents (e.g. contracts) should be assessed for impact prior to system and service changes being approved, and prior to significant new or amended customer requirements being agreed.

Testing should be undertaken at a frequency sufficient to gain assurance that continuity plans are effective, and remain so in the face of changing systems, processes, personnel and business needs. Testing should be a joint involvement between customer and service provider based upon an agreed set of objectives. Test failures should be documented and reviewed to input to a plan for improving the service.

6.4 Budgeting and accounting for IT services

Objective: To budget and account for the cost of service provision.

6.4.1 General

This section covers budgeting and accounting for IT services. In practice, many service providers will be involved in charging for such services. However, since charging is an optional activity, it is not covered by the standard. Service providers are recommended that where charging is in use, the mechanism for doing so is fully defined and understood by all parties.

Responsibility for many of the financial decisions will lie outside the sphere of the service management arena and the requirements for what financial information is to be provided, in what form and at what frequencies may be dictated from outside. The provisions of this section are focused on the practices that should be followed to satisfy the requirements of the standard. However, wider requirements should also be taken into account as they will impact on some of the policies and procedures defined. All accounting practices used should be aligned to the wider accountancy practices of the whole of the service provider's organization.

6.4.2 Policy

There should be a policy on the financial management of services. The policy should define the objectives to be met by budgeting and accounting.

The policy should also define the detail to which budgeting and accounting are performed, taking into consideration the:

a) cost types to be accounted for;

b) apportionment of overhead costs, e.g. flat rate, fixed percentage, or based on the size of the variable element;

c) granularity of the customer's business, e.g. business unit as one unit, subdivided into department, or by locations;

d) rules governing the handling of variances against budgets, e.g. size of variance that will be escalated to senior management;

e) links to service level management.

--`,,```,,,,````-`-`,,`,,`,`,,`---

© ISO/IEC 2005 – All rights reserved

Copyright International Organization for Standardization
Reproduced by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

The level of investment in budgeting and accounting processes should be based on the needs of the customers, service provider and suppliers for financial detail as defined in the policy.

NOTE Service providers operating in a commercial environment might need to invest considerably more time and effort in their financial management. Conversely, for service providers where simple identification of costs is sufficient the financial management can be much simpler.

Budgeting and accounting should be performed by all service providers, whatever their other policies on financial management.

6.4.3 Budgeting

Budgeting should take into account the planned changes to services during the budget period and where budgetary requirements exceed available funds, plan for the management of shortfalls.

Budgeting may take into account factors such as seasonal variations and short term planned changes to service costs and charges.

Cost tracking against the budget should provide early warning of variances against budgets.

There should be a process that manages the implications of variances against budget.

Budgeting and cost tracking should support planning to operate and change the services so that service levels can be maintained throughout the year.

6.4.4 Accounting

Accounting processes should be used to track costs to an agreed level of detail over an agreed period of time.

Decisions about service provision should be based on cost effectiveness comparisons.

Cost models should be able to demonstrate the costs of service provision.

Accounts should demonstrate over and under-spending/recovery; and should allow the reader to understand the costs of low service levels or loss of service.

6.5 Capacity management

Objective: To ensure that the service provider has, at all times, sufficient capacity to meet the current and future agreed demands of customer's business needs.

The current and expected business requirements for services should be understood in terms of what the business will need to enable it to deliver to its customers.

Business predictions and workload estimates should be translated into specific requirements and documented. The result of variations in workload or environment should be predictable; data on current and previous component and resource utilization at an appropriate level should be captured and analysed to support the process.

Capacity management should be the focal point for all performance and capacity issues.

The process should provide direct support to the development of new and changed services by providing sizing and modelling of services.

A capacity plan documenting the actual performance of the infrastructure and the expected requirements should be produced at a suitable frequency taking into account the rate of change in services and service volumes, information in the change management reports and customer business.

--`,,```,,,,````-`-`,,`,,`,`,,`---

© ISO/IEC 2005 – All rights reserved
Copyright International Organization for Standardization
Reproduced by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

It should be produced at least annually. This should document costed options for meeting the business requirements and recommend solutions to ensure achievement of the agreed service level targets as defined in the SLA.

The technical infrastructure and its current and projected capabilities should be well understood.

6.6 Information security management

Objective: To manage information security effectively within all service activities.

6.6.1 General

Information security is the result of a system of policies and procedures designed to identify, control and protect information and any equipment used in connection with its storage, transmission and processing.

The service provider's staff with specialist information security roles should be conversant with ISO/IEC 17799, *Information technology — Security techniques — Code of practice for information security management*.

6.6.2 Identifying and classifying information assets

The service provider should:

a) maintain an inventory of the information assets (for example, computers, communications, environmental equipment, documents and other information) that are necessary to deliver services;

b) classify each asset according to its criticality to the service and the level of protection it requires, and nominate an owner to be accountable for providing that protection;

c) accountability for asset protection should rest with the asset owner, although they may delegate day-to-day security management responsibilities.

6.6.3 Security risk assessment practices

Security risk assessment should:

a) be performed at agreed intervals;

b) be recorded;

c) be maintained during changes (of changing business needs, processes and configurations);

d) help understanding of what could impact a managed service;

e) inform decisions regarding the types of controls to be operated.

6.6.4 Risks to information assets

Risks to information assets should be assessed by reference to:

a) their nature (e.g. software malfunction, operating errors, communications failure);

b) likelihood;

c) potential business impact;

d) past experience.

© ISO/IEC 2005 – All rights reserved

Copyright International Organization for Standardization
Reproduced by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

6.6.5 Security and availability of information

In assessing risks, due regard should be paid to the following:

a) disclosure of sensitive information to unauthorized parties;

b) inaccurate, incomplete or invalid (e.g. fraudulent) information;

c) information being unavailable for use (e.g. due to power failure);

d) physical damage to, or destruction of equipment necessary to provide services.

Account should also be taken of information security policy objectives, the need to meet customers' specified security requirements (e.g. availability levels), and statutory or regulatory requirements that apply.

6.6.6 Controls

In addition to other controls that might be justified and advice contained elsewhere in this part of ISO/IEC 20000 (e.g. on service continuity), service providers should operate the following controls as a matter of good information security management practice:

a) senior management should define their information security policy, communicate it to staff and customers, and act to ensure its effective implementation;

b) information security management roles and responsibilities should be defined, and allocated to post holders;

c) a representative management group (the role might be undertaken by the senior responsible owner) should monitor and maintain the effectiveness of the Information Security Policy;

d) staff with significant security roles should receive information security training;

e) all staff should be made aware of the information security policy;

f) expert help on risk assessment and control implementation should be available;

g) changes should not compromise the effective operation of controls;

h) information security incidents should be reported in line with incident management procedures and a response initiated.

6.6.7 Documents and records

Records should be analysed periodically to provide management with information on:

a) effectiveness of information security policy;

b) emerging trends in information security incidents;

c) input to a plan for improving the service;

d) control over access to information, assets, and systems.

The information security management system should be reliably documented.

--`,,```,,,,````-`-`,,`,,`,`,,`---

© ISO/IEC 2005 – All rights reserved
Copyright International Organization for Standardization
Reproduced by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

7 Relationship processes

7.1 General

Relationship processes describe the two related aspects of Supplier Management and Business Relationship Management. This standard addresses the role of a service provider, who logically fills a role between suppliers, delivering goods or services to the service provider, and the customer who receives services.

Both the suppliers and customer may be internal or external to the service provider's organization. External relationships will be formalized via a contract. Internal relationships will be formalized by a service or internal under-pinning agreement often referred to as an operational level agreement.

Figure 2 shows a simplified representation of the relationships.

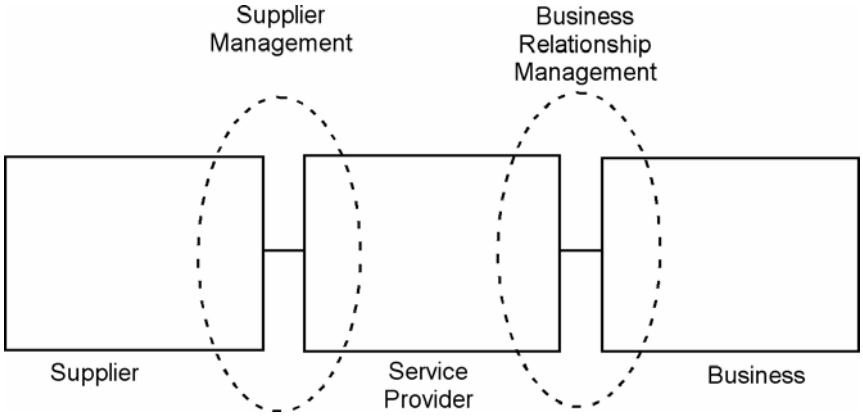

Figure 2 — Relationship processes

As Figure 2 shows, the service provider fills a role within a supply chain, where each step in the chain should be adding benefit, with the service provider receiving services or goods from the supplier and delivering an enhanced service to the customer.

For clarification, within this section the term service provider is always used to describe the organization addressed by this document, irrespective of the role, or direction in the chain, that take in the process being described.

In practice relationships will rarely be this simple, but comprise multiple players, taking roles both as suppliers and customers and with business connections between many of them directly, as well as via the service provider.

The relationship processes should ensure that all parties

a) understand and meet business needs;

b) understand capabilities and constraints;

c) understand responsibilities and obligations.

They should also ensure that customer satisfaction levels are appropriate and that future business needs are communicated and understood.

The scope, roles and responsibilities of the business relationship and the supplier relationship should be defined and agreed. This should include the identification of the stakeholders, contacts and the lines and frequency of communication.

© ISO/IEC 2005 – All rights reserved

Copyright International Organization for Standardization
Reproduced by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

7.2 Business relationship management

Objective: To establish and maintain a good relationship between the service provider and customer based on understanding the customer and their business drivers.

7.2.1 Service reviews

The service provider and customer(s) should hold service reviews, at least annually and before and after major changes. The review should consider past performance, discuss current and projected business needs and propose any changes to the service scope and SLAs. Other stakeholders, e.g. sub-contractors, customers, user groups or other representative bodies may be invited to attend review meetings.

The service provider and customer(s) should also agree on interim review procedures to discuss progress, achievements and issues. These meetings should be scheduled and notified to relevant stakeholders.

The service provider should plan and record all formal meetings, issue records and follow up agreed actions.

The service provider should establish a relationship with their customer such that they would expect to be aware of business needs and major changes and able to prepare to respond to that need.

7.2.2 Service complaints

The service provider and customer(s) should agree on a formal complaints procedure so that there is no ambiguity on what constitutes a complaint and how it should be handled. The service provider should operate a process for taking appropriate action to address issues.

The process should identify the service provider contact for formal complaints.

The service provider should record, investigate, act upon, report and formally close all service complaints.

Outstanding complaints should be reviewed regularly and escalated to higher management if not resolved within time deadlines agreed with the customer(s).

Service providers should periodically analyse the record of complaints to identify trends and report this analysis to customers.

The results of such analysis should be used where appropriate to inform a plan for improving the service.

7.2.3 Customer satisfaction measurement

Customer satisfaction should be measured to enable the service provider to compare performance with customer satisfaction targets and previous surveys. The scope and complexity of the survey should be designed so customers can respond easily and without excessive time being required to complete the survey accurately.

Significant variations in satisfaction levels should be investigated and the reasons understood. Trends or other comparisons should only be made on comparable satisfaction questions and across comparable sampling methods.

The results and conclusions of customer satisfaction surveys should be discussed with the customer. An action plan should be agreed, input to a plan for improving the service and progress reported back to the customer.

Compliments about the service should be documented and reported to the service delivery team.

© ISO/IEC 2005 – All rights reserved
Copyright International Organization for Standardization
Reproduced by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

7.3 Supplier management

Objective: To manage suppliers to ensure the provision of seamless, quality services.

7.3.1 Introduction

Supplier management procedures should ensure that:

a) the supplier understands their obligations to the service provider;

b) legitimate and agreed requirements are met within agreed service levels and scope;

c) changes are managed;

d) business transactions between all parties are recorded;

e) information on performance of all suppliers can be observed and acted upon.

7.3.2 Contract management

The service provider should appoint a manager responsible for contracts and agreements with suppliers. Where a number of staff are engaged in this task, there should be a common process to ensure that information on supplier performance is observed and acted on.

There should be a defined contact within the service provider responsible for the relationship with each supplier.

All supplier contracts should contain a review schedule to assess whether the business objectives for sourcing a service remain valid.

There should be a clearly defined process for managing each contract. The process for contract amendment should also be clearly defined. Any changes to this procedure should be formally notified to all affected suppliers.

A list of contact points within the respective organizations (suppliers' and service provider's) should be maintained. If a contract includes penalties or bonuses, their basis should be clearly stated and compliance to the requirements reported upon.

7.3.3 Service definition

For each service and supplier the service provider should maintain:

a) a definition of services, roles and responsibilities;

b) service scope;

c) contract management process, the authorization levels and a contract exit plan;

d) payment terms if relevant;

e) agreed reporting parameters and records of achieved performance.

© ISO/IEC 2005 – All rights reserved
Copyright International Organization for Standardization
Reproduced by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

7.3.4 Managing multiple suppliers

It should be clear whether the service provider is dealing with all suppliers directly or a lead supplier taking responsibility for sub-contracted suppliers.

The lead supplier should record the names, responsibilities and relationships between all sub-contracted suppliers, and make this available to the service provider if required.

The service provider should obtain evidence that lead suppliers are formally managing sub-contracted providers, guided, where appropriate, by the requirements in ISO/IEC 20000-1.

7.3.5 Contractual disputes management

Both the service provider and the supplier should operate a process for managing disputes and this should be defined or referred to within the contract.

An escalation route should be available for disputes that cannot be resolved through the normal route.

The process should ensure that disputes are recorded, investigated, acted upon and formally closed.

7.3.6 Contract end

The contract management process should include provision for the end of contract – either expected end or early end. It should also provide for the transfer of the service to another organization.

8 Resolution processes

8.1 Background

Incident and problem management are separate processes although they are closely linked. Incident deals with the restoration of service to the users, whereas problem is concerned with identifying and removing the causes of incidents.

8.1.1 Setting priorities

Targets for resolution should be based on priority. Priority should be based on impact and urgency. Impact should be based on the scale of actual or potential damage to the customer's business. Urgency should be based on the time between the problem or incident being detected and the time that the customer's business is impacted.

The scheduling of incident or problem resolution should take into account at least the following:

a) priority;

b) skills available;

c) competing requirements for resources;

d) effort/cost to provide the method of resolution;

e) elapsed time to provide a method of resolution

NOTE Priority is used throughout service management but is central to incident and problem management.

--`,,```,,,,````-`-`,,`,,`,`,,`---

© ISO/IEC 2005 – All rights reserved
Copyright International Organization for Standardization
Reproduced by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

8.1.2 Workarounds

Where appropriate, problem management should develop and maintain workarounds to enable incident management to help service restoration by users of staff.

A known error should only be closed where a corrective change has been successfully applied, or the error is no longer applicable, e.g. because the service is no longer used.

Problem management should have access to information on the business areas affected by problems.

Information on workarounds stored in the knowledge base, their applicability and effectiveness should be stored and maintained.

8.2 Incident management

Objective: To restore agreed service to the business as soon as possible or to respond to service requests

8.2.1 General

NOTE 1 The incident management process may be delivered by a service desk, which acts as the day-to-day contact with the users.

NOTE 2 Incident management should be:

a) both a proactive and reactive process, responding to incidents that affect, or potentially could affect the service;

b) concerned with the restoration of the customers' service, not with determining the cause of incidents.

The incident management process should include the following:

a) call reception, recording , priority assignment, classification;

b) first line resolution or referral;

c) consideration of security issues;

d) incident tracking and lifecycle management;

e) incident verification and closure;

f) first line customer liaison;

g) escalation.

Incidents may be reported by telephone calls, voice mails, visits, letters, faxes or e-mails, or may be recorded directly by users with access to the incident recording system, or by automatic monitoring software.

All incidents should be recorded in a manner that allows relevant information to be retrieved and analysed.

Progress (or lack of it) in resolving incidents should be communicated to those actually or potentially affected. All actions should be recorded on the incident record.

Incident management staff should have access to an up-to-date knowledge base holding information on technical specialists, previous incidents, related problems and known errors, workarounds and checklists that will help in restoring the service to the business.

© ISO/IEC 2005 All rights reserved

Copyright International Organization for Standardization
Reproduced by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Wherever possible, the customer should be provided with the means to continue business, even if only with a degraded service, e.g. by disabling a faulty feature. The motive is to minimize the impact on the customer's business activities. When the cause remains undiagnosed but a workaround is established, details should be recorded for use during continuing problem diagnosis, and when similar incidents recur.

Final closure of an incident should only take place when the initiating user has been given the opportunity to confirm that the incident is now resolved and service restored.

8.2.2 Major incidents

There should be a clear definition of what constitutes a major incident and who is empowered to invoke changes to the normal operation of the incident/problem process.

All major incidents should have a clearly defined responsible manager at all times.

Nomination as manager of a major incident should give the individual authority levels that are adequate to the role of coordinating and controlling all aspects for the resolution. This should include the responsibility for effective escalation and communication across all areas involved in resolution, and to the customers affected by the major incident.

NOTE This level of authority can be temporary, and apply only during that major incident.

The process for a major incident should include a review which will inform a plan for improving the service.

8.3 Problem management

Objective: To minimize disruption to the business by proactive identification and analysis of the causes of incidents and by managing problems to closure.

8.3.1 Scope of problem management

The problem management process should investigate the underlying causes of incidents.

Problem management should proactively prevent the recurrence or replication of incidents or known errors according to the business requirements.

8.3.2 Initiation of problem management

Incidents should be classified to help determine the causes of problems. Classification may reference existing problems and changes.

NOTE On initial registration incidents categorisation will be influenced by other factors also including service, business area affected and symptoms presented.

8.3.3 Known errors

When the problem management investigation has identified the root cause of an incident and a method of resolving the incident, the problem should be classified as a known error.

All known errors should be recorded against the current and potentially affected services in addition to the configuration item suspected of being at fault.

Information on known errors in services being introduced into the live environment should be passed to service management and should be recorded in the knowledge base, together with any workarounds.

A known error should not be closed until after successful resolution.

© ISO/IEC 2005 – All rights reserved
Copyright International Organization for Standardization
Reproduced by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

NOTE The customer or service provider may decide that the resolution is too expensive or not of benefit to the business. If this is the case it should be clearly documented. The known error record should remain open however, since consequential incidents are likely to still occur and may require workarounds and/or require reassessment of the decision to resolve.

8.3.4 Problem resolution

When the root cause has been identified, and a decision to resolve it has been made, the resolution should be progressed via the change management process.

8.3.5 Communication

Information on workarounds, permanent fixes or progress of problems should be communicated to those affected or required to support affected services.

8.3.6 Tracking and escalation

The progress of all problems should be tracked.

All issues should be escalated to the appropriate parties. The process should cover:

a) recording changes to the identities of those responsible for problem resolution during the lifecycle of each problem;

b) identification of incidents that breach service level targets;

c) cascading information to customers and colleagues so that they can take appropriate action to minimize the impact of the unresolved problem;

d) defining the escalation points;

e) the recording of the resources used and any actions taken.

8.3.7 Incident and problem record closure

The record closure procedure should include checking to ensure that:

a) details of resolution have been accurately logged;

b) the cause is categorized to facilitate analysis;

c) if appropriate, both the customer and support staff are aware of the resolution;

d) the customer agrees that the resolution has been achieved;

e) if a resolution is not to be achieved or not possible, the customer is informed.

8.3.8 Problem reviews

Problem reviews should be held where investigation into unresolved, unusual or high-impact problems justifies them. Their purpose is to seek improvements to the process and to prevent recurrence of incidents or mistakes.

--`,,```,,,,````-`-`,,`,,`,`,,`---

© ISO/IEC 2005 – All rights reserved

Copyright International Organization for Standardization
Reproduced by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Problem reviews are typically:

a) reviews of individual incident levels and problem status against service levels;

b) management reviews to highlight those problems that require immediate action;

c) management review to determine and analyse trends and to provide input for other processes, such as user education and training.

8.3.9 Topics for reviews

The reviews should include identification of:

a) trends, e.g. recurring problems and incidents, known errors etc;

b) recurring problems of a particular classification component or location;

c) deficiencies caused by resourcing, training or documentation;

d) non-conformances, e.g. against standards, policies and legislation;

e) known errors in planned releases;

f) staff resource commitment in resolving incidents and problems;

g) recurrence of resolved incidents or problems.

Improvements to the service or the problem management process should be recorded and fed into a plan for improving the service.

The information should be added to the problem management knowledge base.

All relevant documentation should be updated, e.g. user guides and system documentation.

8.3.10 Problem prevention

Proactive problem management should lead to a reduction in incidents and problems. It should include reference to information that assists analysis, such as:

a) asset and configuration;

b) change management;

c) published known error, workaround information from suppliers;

d) historical information on similar problems.

Problem prevention should range from prevention of individual incidents, such as repeated difficulties with a particular feature of a system, through to strategic decisions. The latter can require major expenditure to implement such as investment in a better network, at this level proactive problem management merges into availability management.

Problem prevention also includes information being given to customers that means they do not need to ask for assistance in the future, e.g. preventing incidents caused by lack of user knowledge or training.

© ISO/IEC 2005 – All rights reserved
Copyright International Organization for Standardization
Reproduced by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

9 Control processes

9.1 Configuration management

Objective: To define and control the components of the service and infrastructure and maintain accurate configuration information.

9.1.1 Configuration management planning and implementation

Configuration management should be planned and implemented with change and release management to ensure that the service provider can manage its IT assets and configurations effectively.

Accurate configuration information should be available to support the planning and control of changes as new and updated services and systems are released and distributed. The result should be an efficient system that integrates the service provider's configuration information processes and those of its customers and suppliers, where appropriate.

All major assets and configurations should be accounted for and have a responsible manager who ensures that appropriate protection and control is maintained, e.g. changes are authorized before implementation.

Responsibility for implementing controls may be delegated but accountability should remain with the responsible manager. The responsible manager should be provided with the information necessary to discharge this responsibility, e.g. the person authorising a change may require information on the cost, risks, impact of the change and resources for implementation.

The infrastructure and/or services should have up-to-date configuration management plan(s) that may be stand-alone or form part of other planning documents. They should include or describe:

a) scope, objectives, policies, standards roles and responsibilities;

b) the configuration management processes to define the configuration items in the service(s) and infrastructure, control changes to the configurations, recording and reporting the status of configuration items and verifying the completeness and correctness of configuration items;

c) the requirements for accountability, traceability, auditability, e.g. for security, legal, regulatory or business purposes;

d) configuration control (access, protection, version, build, release controls);

e) interface control process for identifying, recording, and managing the configuration items and information at the common boundary of two or more organizations, e.g. system interfaces, releases;

f) planning and establishing the resources to bring assets and configurations under control and maintain the configuration management system, e.g. training;

g) management of suppliers and sub-contractors performing configuration management.

NOTE An appropriate level of automation should be implemented to ensure that processes do not become either inefficient, error prone or may not be followed at all.

9.1.2 Configuration identification

All configuration items should be uniquely identified and defined by attributes that describe their functional and physical characteristics. Information should be relevant and auditable.

Appropriate markings, or other methods of identification, should be used and recorded in the configuration management database.

© ISO/IEC 2005 All rights reserved
Copyright International Organization for Standardization
Reproduced by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Items to be managed should be identified using established selection criteria and should include:

a) all issues and releases of information systems and software (including third-party software) and related system documentation, e.g. requirements specifications, designs, test reports, release documentation;

b) configuration baselines or build statements for each applicable environment, standard hardware builds and release;

c) master hardcopy and electronic libraries, e.g. definitive software library;

d) configuration management package or tools used;

e) licences;

f) security components, e.g. firewalls;

g) physical assets that need to be tracked for financial asset management or business reasons, e.g. secure magnetic media, equipment;

h) service related documentation, e.g. SLAs, procedures;

i) service supporting facilities, e.g. power to computer room;

j) relationships and dependencies between configuration items.

NOTE Other items that may be considered as configuration items include:

a) other documentation;

b) other assets;

c) other facilities, e.g. site;

d) business units;

e) people.

Appropriate relationships and dependencies between configuration items should be identified to provide the necessary level of control.

Where traceability is required the process should ensure that configuration items can be traced through the full lifecycle, from requirements documents through to release records, e.g. using a traceability matrix.

9.1.3 Configuration control

The process should ensure that only authorized and identifiable configuration items are accepted and recorded from receipt to disposal.

No configuration item should be added, modified, replaced or removed/withdrawn without appropriate controlling documentation, e.g. approved change request, updated release information.

To protect the integrity of systems, services and the infrastructure, configuration items should be held in a suitable and secure environment which:

a) protects them from unauthorized access, change or corruption, e.g. virus;

b) provides a means for disaster recovery;

c) permits the controlled retrieval of a copy of the controlled master, e.g. software.

© ISO/IEC 2005 – All rights reserved
Copyright International Organization for Standardization
Reproduced by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

9.1.4 Configuration status accounting and reporting

Current and accurate configuration records should be maintained to reflect changes in the status, location and versions of configuration items.

Status accounting should provide information on the current and historical data concerned with each configuration item throughout its lifecycle. It should enable changes to configuration items to be tracked through various states, e.g. ordered, received, in acceptance test, live, under change, withdrawn, disposed.

Configuration information should be kept current and made available for planning, decision making and managing changes to the defined configurations.

Where required, configuration information should be accessible for users, customers, suppliers and partners to assist them in their planning and decision making. For example, an external service provider may make configuration information accessible to the customer and other parties to support the other service management processes for the end-to-end service.

Configuration management reports should be available to all relevant parties. The reports should cover the identification and status of the configuration items, their versions and associated documentation.

Reports should cover:

a) latest configuration item versions;

b) location of the configuration item and for software the location of the master versions;

c) interdependencies;

d) version history;

e) status of configuration items that together constitute:

   1) service configuration or system;

   2) a change, baseline, build or release;

   3) version or variant.

9.1.5 Configuration verification and audit

Configuration verification and audit processes, both physical and functional, should be scheduled and a check performed to ensure that adequate processes and resources are in place to:

a) protect the physical configurations and the intellectual capital of the organization;

b) ensure that the service provider is in control of its configurations, master copies and licences;

c) provide confidence that configuration information is accurate, controlled and visible;

d) ensure that a change, a release, a system or an environment conforms to its contracted or specified requirements and that the configuration records are accurate.

Configuration audits should be carried out regularly, before and after major change, after a disaster and at random intervals.

Deficiencies and non-conformities should be recorded, assessed and corrective action initiated, acted upon and fed back to the relevant parties and plan for improving the service.

© ISO/IEC 2005 – All rights reserved

Copyright International Organization for Standardization
Reproduced by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

NOTE Normally there are two types of configuration audits:

a) functional configuration audit: a formal examination to verify that a configuration item has achieved the performance and functional characteristics specified in its configuration documents;

b) physical configuration audit: a formal examination of the “as-built/produced” configuration of a configuration item to verify that it conforms to its product configuration documents.

9.2 Change management

Objective: To ensure all changes are assessed, approved, implemented and reviewed in a controlled manner.

9.2.1 Planning and implementation

The change management processes and procedures should ensure that:

a) changes have a clearly defined and documented scope;

b) only changes that provide business benefit are approved, e.g. commercial, legal, regulatory, statutory;

c) changes are scheduled based on priority and risk;

d) changes to configurations can be verified during change implementation;

e) the time to implement changes is monitored and improved where required

f) it can be demonstrated how a change is:

1) raised, recorded and classified (with references to documents that gave rise to the change);

2) assessed for the impact, urgency, cost, benefits and risk of the changes on the service, customer and release plans;

3) reversed or remedied if unsuccessful;

4) documented, e.g. the change request is linked to affected configuration items and the updated version of the implementation and release plans;

5) approved or rejected by a change authority, depending on the type, size and risk of change;

6) be implemented by the nominated owner within the groups responsible for the components being changed;

7) tested, verified and signed off;

8) closed and reviewed;

9) scheduled, monitored and reported on;

10) linked to incident, problem, other change and configuration item records where appropriate.

The status of changes and scheduled implementation dates should be used as the basis for change and release scheduling.

Scheduling information should be made available to the people affected by the change.

Where an outage can be caused during normal service hours the people affected should agree to the change before implementation.

© ISO/IEC 2005 – All rights reserved
Copyright International Organization for Standardization
Reproduced by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

9.2.2 Closing and reviewing the change request

All changes should be reviewed for success or failure after implementation and any improvements recorded. A post-implementation review should be undertaken for major changes to check that:

a) the change met its objectives;

b) the customers are happy with the results;

c) there have been no unexpected side effects.

Any nonconformity should be recorded and actioned.

Any weaknesses or deficiencies identified in a review of the change management process should be fed into plans for improving the service.

9.2.3 Emergency changes

Emergency changes are sometimes required and where possible the change process should be followed but some details may be documented retrospectively. Where the emergency process bypasses other change management requirements, the change should conform to these requirements as soon as practicable.

Emergency changes should be justified by the implementer and reviewed after the change to verify that it was a true emergency.

9.2.4 Change management reporting, analysis and actions

Change records should be analysed regularly to detect increasing levels of changes, frequently recurring types, emerging trends and other relevant information. The results and conclusions drawn from change analysis should be recorded and acted upon.

10 Release process

10.1 Release management process

Objective: To deliver, distribute and track one or more changes into the live environment.

10.1.1 General

Release management should coordinate the activities of the service provider, many suppliers and the business to plan and deliver a release across a distributed environment.

Good planning and management are essential to package and successfully distribute a release, and to manage the associated impact and risks to the business and IT. The release of affected information systems, infrastructure, services and documentation should be planned with the business.

All associated updates to documentation should be included in the release, e.g. business processes, support documents and service level agreements.

The impact of all new or changed configuration items required to effect the authorized changes should be assessed.

The service provider should ensure that both technical and non technical aspects of the release are considered together.

The release items should be traceable and secure from modification. Only suitably tested and approved releases should be accepted into the live environment.

--`,,```,,,,````-`-`,,`,,`,`,,`---

© ISO/IEC 2005 – All rights reserved

Copyright International Organization for Standardization
Reproduced by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

10.1.2 Release policy

There should be a release policy that includes the:

a) frequency and type of release;

b) roles and responsibilities for release management;

c) authority for the release into acceptance test and production environments;

d) unique identification and description of all releases;

e) approach to grouping changes into a release;

f) approach to automating the build, installation, release distribution processes to aid repeatability and efficiency;

g) verification and acceptance of a release.

10.1.3 Release and roll-out planning

The service provider should work with the business to ensure that the configuration items that are to be released are compatible with each other and with configuration items in the target environment.

Release planning should ensure that the changes to affected information systems, infrastructure, services and documentation are agreed, authorized, scheduled, coordinated and tracked.

The release and roll out should be planned in stages as details of the roll out might not be known initially.

The planning for a release and roll out should typically include:

a) release dates and description of deliverables;

b) related changes, problems and known errors closed or resolved by this release and known errors that have been identified during testing of the release;

c) related processes to implement a release across all business and geographical units;

d) the manner in which the release will be backed-out or remedied if unsuccessful;

e) verification and acceptance process;

f) communication, preparation, documentation and training for customer and support staff;

g) logistics and processes to purchase, store, dispatch, connect, accept and dispose of goods;

h) support resources required to ensure service levels are maintained;

i) the identification of dependencies, related changes and associated risks that might affect the smooth transfer of a release into the acceptance test and production environments;

j) release sign off;

k) schedule of audits of the production environment where required for major upgrades to ensure that the live environment is in the expected state when the release is installed.

--`,,```,,,,````-`-`,,`,,`,`,,`---

© ISO/IEC 2005 – All rights reserved
Copyright International Organization for Standardization
Reproduced by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

10.1.4 Developing or acquiring software

Information systems and software releases from in-house teams, systems builders, system integrators or other organizations should be verified on receipt.

The overall process should be documented in the configuration management plan.

10.1.5 Design, build and configure release

Release and distribution should be designed and implemented to:

a) conform with the service provider's systems architecture, service management and infrastructure standards;

b) ensure the integrity is maintained during build, installation, handling, packaging and delivery;

c) use software libraries and related repositories to manage and control components during the build and release process;

d) risks are clearly identified and remedial action can be taken if required;

e) enable verification that the target platform satisfies prerequisites before installation;

f) enable verification that a release is complete when it reaches its destination.

The outputs from this process should include release notes, installation instructions, installed software and hardware with related configuration baseline.

The outputs from the release should be handed over to the group responsible for testing.

Build, installation, release and distribution processes might be automated to reduce errors, ensure that the process is repeatable and that new releases can be rolled out quickly.

10.1.6 Release verification and acceptance

The end result should be a sign-off on completeness of the whole release package against requirements.

The verification and acceptance processes should:

a) verify that the controlled acceptance test environment matches the requirements of target production environment;

b) ensure that the release is created from versions under configuration management and installed in the acceptance test environment using the planned production process;

c) verify that the appropriate level of testing has been completed, e.g. functional and non-functional testing, business acceptance testing, testing of the build, release, distribution and installation procedures;

d) ensure that the release is tested to the satisfaction of business customers and service provider staff;

e) ensure that the appropriate release authority signs off each stage of acceptance testing;

f) verify that the target platform satisfies the hardware and software prerequisites before installation;

g) verify that a release is complete when it reaches its destination.

© ISO/IEC 2005 – All rights reserved

Copyright International Organization for Standardization
Reproduced by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

10.1.7 Documentation

Appropriate documentation should be available on completion and stored under configuration management against the released configuration item. This documentation should include:

a) support documentation e.g. service level agreements;

b) support documentation, e.g. system overview, installation and support procedures, diagnostic aids, operating and administration instructions;

c) build, release, installation and distribution processes;

d) contingency and back-out plans;

e) training schedule for service management, support staff and customers;

f) a configuration baseline for the release including associated configuration items such as system documentation, test environments, test documentation, versions of build and development tools;

g) related changes, problems and known errors;

h) evidence of release authorization and related evidence of verification and acceptance.

A system or service which does not completely conform to its specified requirements should be identified and recorded through configuration management and problem management prior to going live.

Information on known errors should be communicated to incident management.

If the release is rejected, delayed or cancelled, change management should be informed.

10.1.8 Roll-out, distribution and installation

The roll out plan should be reviewed and detail added as necessary to ensure that all necessary activities will be performed.

It is important that the release is delivered safely to its destination in its expected state. The roll-out, distribution and installation processes should ensure that:

a) all hardware and software storage areas are secure;

b) there are appropriate procedures for the storage, despatch, receipt and disposal of goods;

c) installation, environmental, electrical and facilities checks are planned and completed;

d) that business and service provider staff are notified of new releases;

e) redundant products, services and licences are decommissioned.

After software distribution over a network it is essential to check that the release is complete and operational when it reaches its destination.

After a successful installation the asset and configuration management records should be updated with the location and the owner of the hardware and software.

An installation customer acceptance and satisfaction questionnaire may be used to record success or failure. Results of any customer surveys should be fed back to business relationship management.

© ISO/IEC 2005 – All rights reserved
Copyright International Organization for Standardization
Reproduced by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

10.1.9 Post release and roll-out

The number of incidents related to the release in the period immediately following a roll-out should be measured and analysed to assess their impact on the business, operations and support staff resources.

The change management process should include a post-implementation review.

Recommendations should be fed into a plan for improving the service.

© ISO/IEC 2005 – All rights reserved

Copyright International Organization for Standardization
Reproduced by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Bibliography

[1] ISO/IEC 20000-1, *Information technology — Service management — Part 1: Specification*

[2] ISO/IEC 17799, *Information technology — Security techniques — Code of practice for information security management*

[3] ISO/IEC 12207, *Information technology — Software life cycle processes*

[4] ISO/IEC TR 15271, *Information technology — Guide for ISO/IEC 12207 (Software life cycle processes)*

[5] ISO/IEC TR 16326, *Software engineering — Guide for the application of ISO/IEC 12207 to project management*

[6] ISO/IEC 15288, *Systems engineering — System life cycle processes*

[7] ISO/IEC TR 19760, *Systems engineering — A guide for the application of ISO/IEC 15288 (System life cycle processes)*

[8] ISO/IEC 15504-1, *Information technology — Process assessment — Part 1: Concepts and vocabulary*

[9] ISO/IEC 15504-2, *Information technology — Process assessment — Part 2: Performing an assessment*

[10] ISO/IEC 15504-3, *Information technology — Process assessment — Part 3: Guidance on performing an assessment*

[11] ISO/IEC 15504-4, *Information technology — Process assessment — Part 4: Guidance on use for process improvement and process capability determination*

[12] ISO/IEC 15504-5, *Information technology — Process assessment — Part 5: An exemplar Process Assessment Model*

[13] ISO 10007, *Quality management systems — Guidelines for configuration management*

[14] ISO 9000, *Quality management systems — Fundamentals and vocabulary*

[15] ISO 9001, *Quality management systems — Requirements*

[16] ISO/IEC 90003, *Software engineering — Guidelines for the application of ISO 9001:2000 to computer software*

© ISO/IEC 2005 – All rights reserved
Copyright International Organization for Standardization
Reproduced by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

--`,,```,,,,````-`-`,,`,,`,`,,`---

Copyright International Organization for Standardization
Reproduced by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

ICS 03.080.99; 35.020

Price based on 34 pages

© ISO/IEC 2005 – All rights reserved
Copyright International Organization for Standardization
Reproduced by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale