

IT service management

Part 1: Specification for service management

ICS 35.020

Committees responsible for this British Standard

The preparation of this British Standard was entrusted to Technical Committee BDD/3, Information services management, upon which the following bodies were represented:

British Broadcasting Corporation (BBC)

British Computer Society (BCS)

Office of Government Commerce (OGC)

IT Service Management Forum (itSMF)

Co-opted Members

This British Standard, having been prepared under the direction of the DISC Board, was published under the authority of the Standards Policy and Strategy Committee on 27 September 2002

© BSI 27 September 2002

The following BSI references relate to the work on this British Standard:

Committee reference BDD/3
Draft for comment 02/683006

ISBN 0 580 40470 6

Amendments issued since publication

Amd. No.	Date	Comments

Contents

	Page
Committees responsible	Inside front cover
Foreword	ii
<hr/>	
1 Scope	2
2 Terms and definitions	2
3 Requirements for a management system	4
4 Planning and implementing service management	5
5 Planning and implementing new or changed services	7
6 Service delivery process	7
7 Relationship processes	9
8 Resolution processes	11
9 Control processes	11
10 Release process	12
<hr/>	
Bibliography	13
<hr/>	
Figure 1 — Plan-Do-Check-Act methodology for service management processes	1
Figure 2 — Service management process	2
Figure 3 — Example of relationship between service providers and suppliers	10
<hr/>	

Foreword

BS 15000-1 has been prepared by Technical Committee BDD/3 and is based on the knowledge and experience gained by experts working in the field. It supersedes BS 15000:2000, which is withdrawn.

BS 15000 is issued in two parts:

- *Part 1: Specification for service management;*
- *Part 2: Code of practice for service management.*

This British Standard should be used in conjunction with BS 15000-2, the code of practice associated with this specification. It may also be used in conjunction with DISC PD 0005, *Management Overview*, and DISC PD 0015, *IT service Management — Self-assessment Workbook*. DISC PD 0015 is a checklist that complements this specification. This workbook has been designed to assist organizations to assess the extent to which their IT services conform to the specified requirements.

A standard forms part of a trade description when cited by number or when compliance with it is claimed. Even if a standard does not specifically require marking with its number, organizations often refer to it in documentation. Such marking or reference constitutes a unilateral claim that the product, process or service conforms to all the relevant requirements of the standard cited. The person making the claim is legally responsible in the UK under the Trade Descriptions Act 1968 [1].

It is assumed that the execution of the provisions of this standard is entrusted to appropriately qualified and competent people.

A British Standard does not purport to include all necessary provisions of a contract. Users of British Standards are responsible for their correct application.

Attention is drawn to the following statutory regulations:

- Trade Descriptions Act 1968 [1];
- Data Protection Act 1998 [2];
- Computer Misuse Act 1990 [3];
- Copyright, Designs and Patent Act 1988 [4].

BSI Committee BDD/3, whose constitution is shown in this British Standard, takes collective responsibility for its preparation under the authority of the Standards Board. The Committee wishes to acknowledge the personal contributions of:

Jenny Dugmore	Service Matters Ltd.
Lynda Cooper	Xansa
Ivor Evans	IT Service Improvement Ltd.
Hilary Faul	BBC Technology Ltd.
John Groom	Office of Government Commerce (OGC)
Shirley Lacy	ConnectSphere Ltd and representative of the BCS
Aidan Lawes	IT Service Management Forum (itSMF)
Ivor Macfarlane	IT Service Improvement Ltd.
Don Page	Marval Software Ltd.

Compliance with a British Standard does not of itself confer immunity from legal obligations.

Summary of pages

This document comprises a front cover, an inside front cover, pages i and ii, pages 1 to 13 and a back cover.

The BSI copyright displayed in this document indicates when the document was last issued.

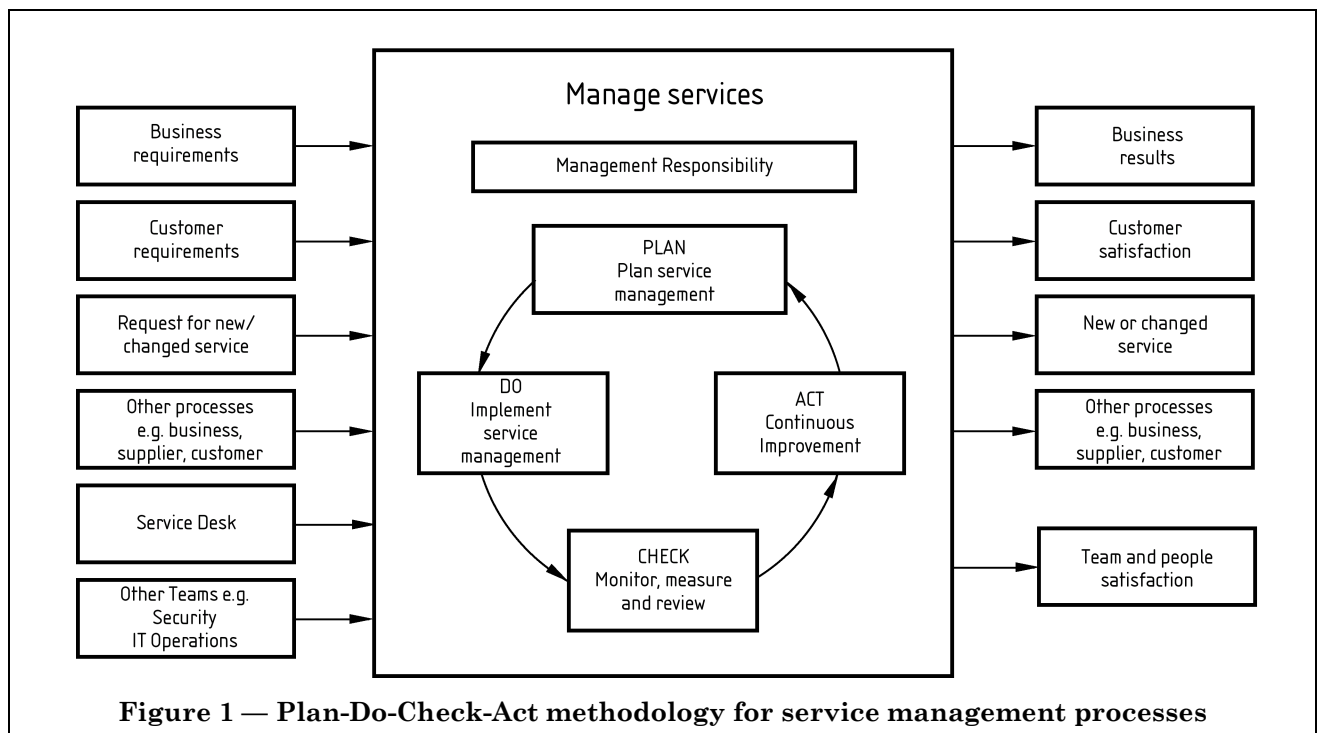
Introduction

This standard promotes the adoption of an integrated process approach to effectively deliver managed services to meet the business and customer requirements. For an organization to function effectively it has to identify and manage numerous linked activities. An activity using resources, and managed in order to enable the transformation of inputs into outputs, can be considered as a process. Often the output from one process forms an input to another.

Co-ordinated integration and implementation of the service management processes provides the ongoing control, greater efficiency and opportunities for continuous improvement. Performing the activities and processes requires people in the service desk, service support, service delivery and operations teams to be well organized and co-ordinated. Appropriate tools are also required to ensure that the processes are effective and efficient.

NOTE The methodology known as Plan-Do-Check-Act (PDCA) can be applied to all processes. PDCA can be described as follows:

- 1) Plan: establish the objectives and processes necessary to deliver results in accordance with customer requirements and the organization's policies;
- 2) Do: implement the processes;
- 3) Check: monitor and measure processes and services against policies, objectives and requirements and report the results;
- 4) Act: take actions to continually improve performance.

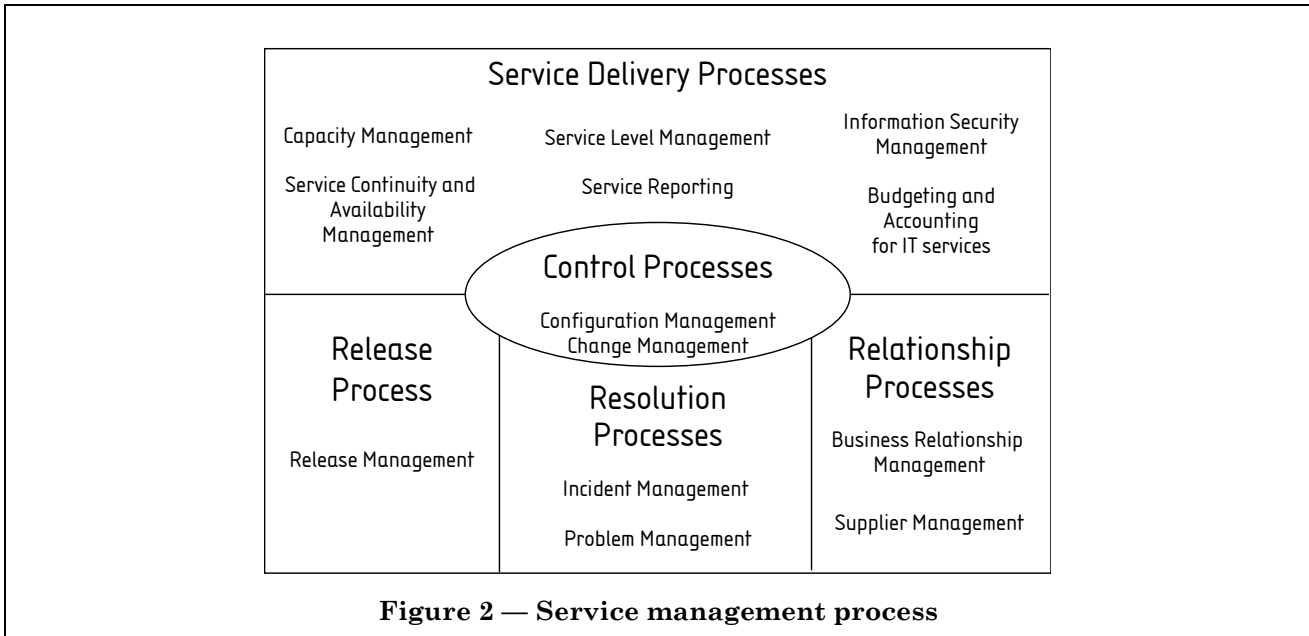


The model shown in Figure 1 illustrates the process and process linkages presented in Clause 5, Clause 6 and Clause 7.

1 Scope

This specification defines the requirements for an organization to deliver managed services of an acceptable quality for its customers. It may be used:

- a) by businesses that are going out to tender for their services;
- b) by businesses that require a consistent approach by all service providers in a supply chain;
- c) by service providers to benchmark their IT service management;
- d) as the basis for an assessment which may lead to a formal certification;
- e) by an organization who needs to demonstrate the ability to provide services that meet customer requirements; and
- f) by an organization which aims to improve service through the effective application of processes to monitor and improve service quality.



This standard specifies a number of closely related service management processes, as shown in Figure 1.

The relationships between the processes depend on the application within an organization and are generally too complex to model and therefore relationships between processes are not shown in this diagram.

The list of objectives and controls contained in this specification are not exhaustive, and an organization may consider that additional objectives and controls are necessary to meet their particular business needs. The nature of the business relationship between the service provider and business will determine how the requirements in this Standard are implemented in order to meet the overall objective.

2 Terms and definitions

For the purposes of this part of BS 15000, the following terms and definitions apply.

2.1

availability

ability of a component or service to perform its required function at a stated instant or over a stated period of time

NOTE Availability is usually expressed as a ratio of the time that the service is actually available for use by the business to the agreed service hours.

2.2**baseline**

snapshot of the state of a service or an individual configuration item at a point in time

2.3**change record**

record containing details of which configuration items (see 2.4) are affected and how they are affected by an authorized change

2.4**configuration item (CI)**

component of an infrastructure or an item which is, or will be, under the control of configuration management

NOTE Configuration items may vary widely in complexity, size and type, ranging from an entire system including all hardware, software and documentation, to a single module or a minor hardware component.

2.5**configuration management database (CMDB)**

database containing all the relevant details of each configuration items and details of the important relationships between them

2.6**document**

information in readable form, including computer data, which is created or received and maintained as evidence of the service provider's intentions with regards to service management

NOTE 1 In this standard, records are distinguished from documents by the fact that they function as evidence of activities, rather than evidence of intentions.

NOTE 2 Examples of documents include policy statements, plans, procedures, service level agreements and contracts.

2.7**incident**

any event which is not part of the standard operation of a service and which causes or may cause an interruption to, or a reduction in, the quality of that service

NOTE This may include request questions such as "How do I...?" calls.

2.8**problem**

unknown underlying cause of one or more incidents

2.9**record**

information in readable form, including computer data, which is created or received and maintained by the service provider as evidence of the performance of service management activities

NOTE 1 In this standard, records are distinguished from documents by the fact that they function as evidence of activities, rather than evidence of intentions.

NOTE 2 Examples of records include audit reports, requests for change, incident reports, individual training records and invoices sent to customers.

2.10**release**

collection of new and/or changed configuration items which are tested and introduced into the live environment together

2.11**request for change**

form or screen used to record details of a request for a change to any configuration item within a service or infrastructure

2.12

service desk

customer facing support group who do a high proportion of the total support work

2.13

service level agreement (SLA)

written agreement between a service provider and a customer that documents services and agreed service levels

2.14

service management

management of services to meet the business requirements

3 Requirements for a 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

Through leadership and actions, top management shall provide evidence of its commitment to developing, implementing and improving its service management capability within the context of the organization's business and customers' requirements. Management shall:

- a) establish the service management policy, objectives and plans;
- b) communicate the importance of meeting the service management objectives and the need for continual improvement;
- c) ensure that customer requirements are determined and are met with the aim of improving customer satisfaction;
- d) appoint a member of management responsible for the co-ordination and management of all services;
- e) determine and provide resources to plan, implement, monitor, review and improve service delivery and management e.g. recruit appropriate staff, manage staff turnover;
- f) manage risks to the service management organization and services; and
- g) conduct reviews of service management, at planned intervals, to ensure continuing suitability, adequacy and effectiveness.

3.2 Documentation requirements

Service providers shall provide documentation and records to ensure effective planning, operation and control of service management. This shall include:

- a) documented service management policies and plans;
- b) documented service level agreements;
- c) documented processes and procedures required by this standard; and
- d) records required by this standard.

Procedures and responsibilities shall be established for the creation, review, approval, maintenance and control of the various types of documents and records.

NOTE The documentation can be in any form or type of medium.

3.3 Competence, awareness and training

All service management roles and responsibilities shall be defined and maintained together with the competencies required to execute them effectively. Staff competencies and training needs shall be reviewed and managed to enable staff to perform their role effectively.

Top management shall ensure that its employees are aware of the relevance and importance of their activities and how they contribute to the achievement of the service management objectives.

4 Planning and implementing service management

NOTE See also Introduction.

4.1 Plan service management (Plan)

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

Service management shall be planned. The plans shall at a minimum define:

- a) the scope of service management within the organization;
- b) the objectives and requirements that are to be achieved by service management;
- c) the processes that are to be executed;
- d) the framework of management roles and responsibilities, including the process owner and management of third party suppliers;
- e) the interfaces between service management processes and the manner in which the activities 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) the approach for interfacing to projects that are creating or modifying services;
- h) the resources, facilities and budget necessary to achieve the defined objectives;
- i) tools as appropriate to support the processes; and
- j) how the quality of the service will be managed, audited and improved.

There shall be clear management direction and documented responsibilities for reviewing, authorising, communicating, implementing and maintaining the plans.

Any process specific plans produced shall be compatible with this service management plan.

4.2 Implement service management and provide the services (Do)

Objective: To implement the service management objectives and plan.

The organization shall implement the service management plan to manage and deliver the services, including:

- a) allocation of funds and budgets;
- b) allocation of roles and responsibilities;
- c) documenting and maintaining the policies, plans, procedures and definitions for each process or set of processes;
- d) identification and management of risks to the service;
- e) managing teams, e.g. recruiting and developing appropriate staff and managing staff continuity;
- f) managing facilities and budget;
- g) managing the teams including service desk and operations;
- h) reporting progress against the plans; and
- i) co-ordination of service management processes.

4.3 Monitoring, measuring and reviewing (Check)

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

The organization shall apply suitable methods for monitoring and, where applicable, measurement of the service management processes. These methods shall demonstrate the ability of the processes to achieve planned results.

Management shall conduct reviews at planned intervals to determine whether the service management requirements:

- a) conform with the service management plan and to the requirements of this standard; and
- b) are effectively implemented and maintained.

An audit programme shall be planned, taking into consideration the status and importance of the processes and areas to be audited, as well as the results of previous audits. The audit criteria, scope, frequency and methods shall be defined. The selection of auditors and conduct of audits shall ensure objectivity and impartiality of the audit process. Auditors shall not audit their own work.

The objective of service management reviews, assessments and audits shall be recorded together with the findings of such audits and reviews and any remedial actions identified. Any significant areas of non-compliance or concern shall be communicated to relevant parties.

4.4 Continuous improvement (Act)

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

There shall be a published policy on service improvement. Any non-compliance with the standard or the service management plans shall be remedied. Roles and responsibilities for service improvement activities shall be clearly defined.

All suggested service improvements shall be assessed, recorded, prioritized and authorized. A service improvement plan shall be used to control the activity.

The organization shall have a process in place to identify, measure, report and manage improvement activities on an ongoing basis. This shall include:

- a) improvements to an individual process that can be implemented by the process owner with the usual staff resources, e.g. performing individual corrective and preventive actions; and
- b) improvements across the organization or across more than one process.

The organization shall perform activities to:

- 1) collect and analyse data to baseline and benchmark the organization's capability to manage and deliver service management;
- 2) identify, plan and implement improvements;
- 3) consult with all parties involved;
- 4) set targets for improvements in quality, costs and resource utilization;
- 5) consider relevant inputs about improvements from all the service management processes;
- 6) measure, report and communicate the service improvements;
- 7) revise the service management policies, plans and procedures where necessary; and
- 8) ensure that all approved actions are delivered and that they achieve their intended objectives.

Major service improvements shall be managed as a project or several projects.

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 right cost and service quality.

Proposals for new or changed services shall consider the cost, organizational, technical and commercial impact that could result from service delivery and management.

The implementation of new or changed services, including closure of a service, shall be planned and approved through formal change management. The planning and implementation shall include adequate funding and resources to make the changes needed for service delivery and management. The plans shall include:

- a) the roles and responsibilities for implementing, operating and maintaining the new or changed service including activities to be performed by customers and third party suppliers;
- b) changes to the existing service management framework and services;
- c) communication to the relevant parties;
- d) new or changed contracts and agreements to align with the changes in business need;
- e) manpower and recruitment requirements;
- f) skills and training requirements, e.g. end users, technical support;
- g) processes, measures, methods and tools to be used in connection with the new or changed service, e.g. capacity management, financial management;
- h) budgets and time-scales;
- i) service acceptance criteria; and
- j) the expected outcomes from operating the new service expressed in measurable terms.

New or changed services shall be accepted by the service provider before being implemented into the live environment.

The service provider shall report on the outcomes achieved by the new or changed service against those planned following its implementation. A post implementation review comparing actual outcomes against those planned, shall be performed through the change management process and the results reported to the relevant parties.

6 Service delivery process

6.1 Service level management

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

The full range of services to be provided together with the corresponding service level targets and workload characteristics shall be agreed by the parties and recorded. Each service provided shall be defined, agreed and documented in one or more service level agreements (SLAs). SLAs, together with supporting service agreements, third party contracts and corresponding procedures, shall be agreed by all relevant parties and recorded.

The SLAs shall be under change control.

The SLAs shall be maintained by regular reviews by the parties to ensure that they are up-to-date and remain effective over time.

Service levels shall be monitored and reported against targets, showing both current and trend information. The reasons for non-conformance shall be reported and reviewed and shall provide input to the service improvement plan.

6.2 Service reporting

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

There shall be a clear description of each service report including its identity, purpose, audience and details of the data source.

Service reports shall be produced to meet identified needs and customer requirements. Typically service reporting shall include:

- a) performance against service level targets;
- b) non-compliance and issues, e.g. against the SLA, security breach;
- c) workload characteristics, e.g. volume, resource utilisation;
- d) performance reporting following major events, e.g. major incidents and changes;
- e) trend information;
- f) satisfaction analysis.

Management decisions and corrective actions shall take into consideration the findings in the service reports and shall be communicated to relevant parties.

6.3 Availability and service continuity management

Objective: To ensure that agreed obligations to customers can be met in all circumstances.

Availability and service continuity requirements shall be identified on the basis of business plans, SLAs and risk assessments. Requirements shall include access rights and response times as well as end to end availability of system components.

Availability and service continuity plans shall be developed and reviewed at least annually to ensure that requirements are met as agreed in all circumstances from normal through to a major loss of service. These plans shall be maintained to ensure that they reflect agreed changes required by the business.

The change management process shall assess the impact of any change on the availability and service continuity plan.

Availability shall be measured and recorded.

Unplanned non-availability shall be investigated and appropriate actions taken. Where possible, potential issues shall be predicted and preventive action taken.

Service continuity plans, contact lists and the configuration management database shall be available when normal office access is prevented. The service continuity plan shall include the return to normal working.

The service continuity plan shall be tested in accordance with business needs.

All continuity tests shall be recorded and test failures shall be formulated into action plans.

6.4 Budgeting and accounting for IT services

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

NOTE This section covers budgeting and accounting for IT services. In practice, many organizations will be involved in charging for such services. However, since charging is an optional activity, it is not covered by the standard. Organizations are recommended that where charging is in use, the mechanism for doing so is fully defined and understood by all parties. All accounting practices in use should be aligned to the wider accountancy practices of the organisation.

There shall be clear policies and procedures for:

- a) budgeting, and accounting for all components including IT assets, shared resources, overheads, third-party supplied service, people, insurance and licences;
- b) apportioning and allocating all indirect costs to relevant services;
- c) effective financial control and authorization.

Costs shall be budgeted in sufficient detail to enable effective financial control and decision making.

The service provider shall monitor and report costs against the budget, review the financial forecasts and manage costs accordingly.

Changes to services shall be costed and approved through the change management process.

6.5 Capacity management

Objective: To ensure that the organization has, at all times, sufficient capacity to meet the current and future agreed demands of the business.

Capacity management shall produce and maintain a capacity plan. Capacity management shall address the business needs and include:

- a) current and predicted capacity and performance requirements;
- b) identified time-scales, thresholds and costs for service upgrades;
- c) evaluation of effects of anticipated service upgrades, requests for change, new technologies and techniques on capacity;
- d) predicted impact of external changes, e.g. legislative;
- e) data and processes to enable predictive analysis.

Methods, procedures and techniques shall be identified to monitor service capacity, tune service performance and provide adequate capacity.

6.6 Information security management

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

NOTE BS ISO/IEC 17799 (BS 7799-1) provides guidance on information security management. Implementation of the requirements in this specification may not satisfy all the requirements that are necessary to obtain certification against BS 7799-2. Organizations certified to BS 7799 will satisfy the security requirements within BS 15000-1.

Management with appropriate authority shall approve an information security policy that shall be communicated to all relevant personnel and customers where appropriate.

Appropriate security controls shall operate to:

- a) implement the requirements of the information security policy;
- b) manage risks associated with access to the service or systems.

Security controls shall be documented. The documentation shall describe the risks to which the controls relate, and the manner of operation and maintenance of the controls. The impact of changes on controls shall be assessed before changes are implemented.

Arrangements that involve third-party access to information systems and services shall be based on a formal agreement that defines all necessary security requirements.

Security incidents shall be reported and recorded in line with incident management procedure as soon as possible. Procedures shall be in place to ensure that all security incidents are investigated, and management action taken. Mechanisms shall be in place to enable the types, volumes and impacts of security incidents and malfunctions to be quantified and monitored, and to provide input to the service improvement plan.

7 Relationship processes

7.1 Business relationship management

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

The service provider shall identify and document the stakeholders and customers of the services.

The service provider and customer shall attend a service review to discuss any changes to the service scope, SLA, contract (if present) or the business needs at least annually and shall hold interim meetings at agreed intervals to discuss performance, achievements, issues and action plans. These meetings shall be documented. Other stakeholders in the service may also be invited to the meetings. Changes to the contract(s), if present, and SLA(s) shall follow from these meetings as appropriate. These changes shall be subject to the change management process.

The service provider shall remain aware of business needs and major changes in order to prepare to respond to these needs.

There shall be a complaint procedure. The definition of a formal service complaint shall be agreed with the customer. All formal service complaints shall be recorded by the service provider, investigated, acted upon, reported and formally closed. Where a complaint is not resolved through the normal channels, escalation shall be available to the customer.

The service provider shall have a named individual or individuals who are responsible for managing customer satisfaction and the whole business relationship process. A process shall exist for obtaining and acting upon feedback from regular customer satisfaction measurements.

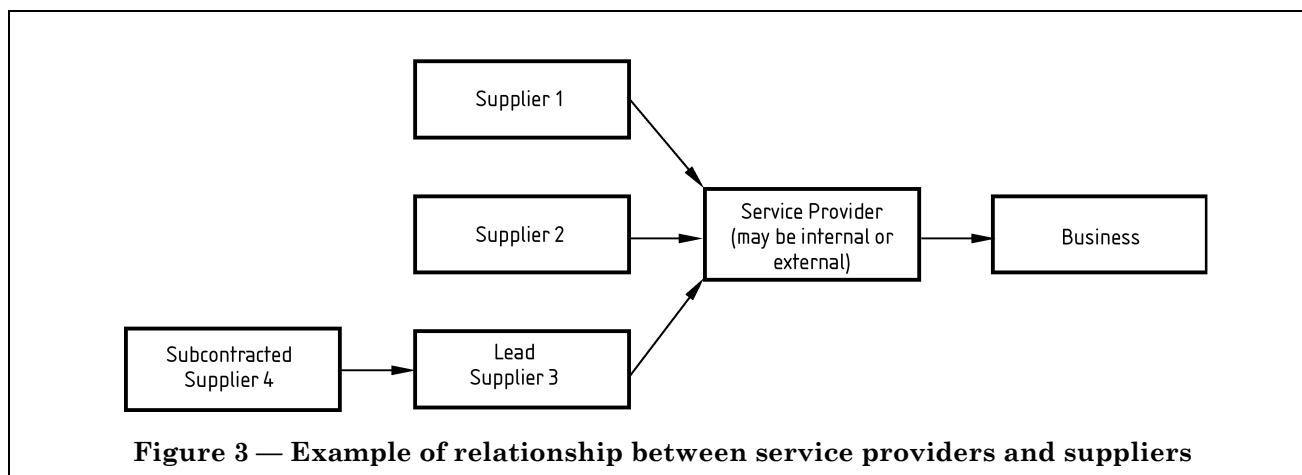
Actions for improvement identified during this process shall be recorded and input into the service improvement plan.

7.2 Supplier management

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

NOTE 1 The scope of this standard excludes the procurement of the suppliers.

NOTE 2 Third party suppliers may be used by the service provider for provision of some part of the service. It is the service provider who needs to demonstrate conformity to these supplier management processes. Complex relationships may be present as demonstrated in the diagram below which is used as an example:



The service provider shall have documented supplier management processes and shall name a contract manager responsible for each supplier.

The requirements, scope, level of service and communication processes to be provided by the supplier(s) shall be documented in SLAs or other documents and agreed by all parties.

SLAs with the suppliers shall be aligned with the SLA(s) with the business.

The interfaces between processes used by each party shall be documented and agreed.

All roles and relationships between lead and subcontracted suppliers shall be clearly documented. Lead suppliers shall be able to demonstrate processes to ensure that subcontracted suppliers meet contractual requirements.

A process shall be in place for a major review of the contract or formal agreement at least annually to ensure that business needs and contractual obligations are still being met.

Changes to the contract(s), if present, and SLA(s) shall follow from these reviews as appropriate or at other times as required. Any changes shall be subject to the change management process.

A formal process shall exist to deal with contractual disputes.

A process shall be in place to deal with the expected end of service, early end of the service or transfer of service to another party.

Performance against service level targets shall be monitored and reviewed. Actions for improvement identified during this process shall be recorded and input into the service improvement plan.

8 Resolution processes

8.1 Incident management

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

All incidents shall be recorded.

Procedures shall be adopted to manage the impact of service incidents. Procedures shall define the recording, prioritization, business impact, classification, updating, escalation, resolution and formal closure of all incidents.

The customer shall be kept informed of the progress of their reported incident or service request and alerted in advance if their service levels cannot be met and an action agreed.

All staff involved in incident management shall have access to relevant information such as known errors, problem resolutions and the configuration management database (CMDB).

Major incidents shall be classified and managed according to a defined process.

8.2 Problem management

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

All identified problems shall be recorded.

Procedures shall be adopted to identify, minimize or avoid the impact of incidents and problems. They shall define the recording, classification, updating, escalation, resolution and closure of all problems.

Preventive action will be taken to reduce potential problems, e.g. following trend analysis of incident volumes and types.

Changes required in order to correct the underlying cause of problems shall be passed to the change management process.

Problem resolution shall be monitored, reviewed and reported on for effectiveness.

Problem management shall be responsible for ensuring up-to-date information on known errors and corrected problems is available to incident management.

Actions for improvement identified during this process shall be recorded and input into the service improvement plan.

9 Control processes

9.1 Configuration management

NOTE 1 Financial asset accounting falls outside the scope of this section.

NOTE 2 BS EN ISO 10007 provides further guidelines on configuration management.

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

There shall be an integrated approach to change and configuration management planning.

The service provider shall define the interface to financial asset accounting processes.

There shall be a policy on what is defined as a configuration item and its constituent components. The information to be recorded for each item shall be defined and shall include the relationships and documentation necessary for effective service management. Configuration management shall provide the mechanisms for identifying, controlling and tracking versions of identifiable components of the service and infrastructure. The degree of control shall be sufficient to meet the business needs, risk of failure and service criticality.

Configuration management shall provide information to the change management process on the impact of a requested change on the service and infrastructure configurations.

Changes to configuration items shall be traceable and auditable where appropriate, e.g. for changes and movements of software and hardware.

Configuration control procedures shall ensure that the integrity of systems, services and service components are maintained.

A baseline of the appropriate configuration items shall be taken before a release to the live environment. Master copies of digital configuration items shall be controlled in secure physical or electronic libraries and reference to the configuration records, e.g. software, testing products, support documents.

All configuration items shall be uniquely identifiable and recorded in a CMDB to which update access shall be strictly controlled. The CMDB shall be actively managed and verified to ensure its reliability and accuracy. The status to configuration items, their versions, location, related changes and problems and associated documentation shall be visible to those who require it.

Configuration audit procedures shall include recording deficiencies and instigating corrective actions and reporting on the outcome.

9.2 Change management

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

Service and infrastructure changes shall have a clearly defined and documented scope.

All requests for change shall be recorded and classified, e.g. urgent, emergency, major, minor.

Requests for changes shall be assessed for their risk, impact and business benefit. The change management process shall include the manner in which the change shall be reversed or remedied if unsuccessful.

Changes shall be approved and then checked, and shall be implemented in a controlled manner. All changes shall be reviewed for success and any actions taken after implementation.

There shall be policies and procedures to control the authorization and implementation of emergency changes.

The scheduled implementation dates of changes shall be used as the basis for change and release scheduling. A forward schedule of change shall be maintained and communicated to relevant parties.

Change records shall 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 shall be recorded.

Actions for improvement identified from change management shall be recorded and input into the service improvement plan.

10 Release process

10.1 Release management

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

The release policy stating the frequency and type of releases shall be documented and agreed.

The service provider shall plan with the business the release of services, systems, software and hardware. Plans on how to roll out the release shall be agreed and authorized by all relevant parties, e.g. customers, users, operations and support staff. The process shall include the manner in which the release shall be backed-out or remedied if unsuccessful. Plans shall record the release dates and deliverables and refer to related change requests, known errors and problems. They shall be communicated to incident management.

Requests for change shall be assessed for their impact on release plans. Release management procedures shall include the updating and changing of configuration information and change records. Emergency releases shall be managed according to a defined process that interfaces to the emergency change management process.

A controlled acceptance test environment shall be established to build and test all releases prior to distribution.

Release and distribution shall be designed and implemented so that the integrity of hardware and software is maintained during installation, handling, packaging and delivery.

Success and failure of releases shall be measured. Measurements shall include incidents related to a release in the period following a release. Analysis shall include assessment of the impact on the business, IT operations and support staff resources, and shall provide input to the service improvement plan.

Bibliography

Standards publications

BS 15000-2:2002, *IT service management — Part 2: Code of practice for IT service management*.

DISC PD 0005:2003, *Management Overview*.¹⁾

DISC PD 0015:2002, *IT service management — Self-assessment workbook*.

BS EN ISO 10007:1997, *Quality management — Guidelines for configuration management*.

BS 7799-1:2000, *Information technology — Code of practice for information security management*.

BS 7799-2:2002, *Information security management systems — Specification with guidance for use*.

BS 8600:1999, *Complaints management systems*.

Non-standards publications

[1] GREAT BRITAIN. Trade Descriptions Act 1968. London: The Stationery Office.

[2] GREAT BRITAIN. Data Protection Act 1998. London: The Stationery Office.

[3] GREAT BRITAIN. Computer Misuse Act 1990. London: The Stationery Office.

[4] GREAT BRITAIN. Copyright, Designs and Patent Act 1988. London: The Stationery Office.

Other sources of information

The IT infrastructure library ITIL®²⁾ published by The Stationery Office, visit www.itil.co.uk.

¹⁾ To be published.

²⁾ ITIL® (IT infrastructure library) is a registered trade mark of OGC (the Office of Government Commerce), Rosebery Court, St. Andrew's Business Park, Norwich, Norfolk, NR7 0HS. This information is given for the convenience of users of this standard and does not constitute and endorsement by BSI of this product.

BSI — British Standards Institution

BSI is the independent national body responsible for preparing British Standards. It presents the UK view on standards in Europe and at the international level. It is incorporated by Royal Charter.

Revisions

British Standards are updated by amendment or revision. Users of British Standards should make sure that they possess the latest amendments or editions.

It is the constant aim of BSI to improve the quality of our products and services. We would be grateful if anyone finding an inaccuracy or ambiguity while using this British Standard would inform the Secretary of the technical committee responsible, the identity of which can be found on the inside front cover. Tel: +44 (0)20 8996 9000. Fax: +44 (0)20 8996 7400.

BSI offers members an individual updating service called PLUS which ensures that subscribers automatically receive the latest editions of standards.

Buying standards

Orders for all BSI, international and foreign standards publications should be addressed to Customer Services. Tel: +44 (0)20 8996 9001. Fax: +44 (0)20 8996 7001. Email: orders@bsi-global.com. Standards are also available from the BSI website at <http://www.bsi-global.com>.

In response to orders for international standards, it is BSI policy to supply the BSI implementation of those that have been published as British Standards, unless otherwise requested.

Information on standards

BSI provides a wide range of information on national, European and international standards through its Library and its Technical Help to Exporters Service. Various BSI electronic information services are also available which give details on all its products and services. Contact the Information Centre. Tel: +44 (0)20 8996 7111. Fax: +44 (0)20 8996 7048. Email: info@bsi-global.com.

Subscribing members of BSI are kept up to date with standards developments and receive substantial discounts on the purchase price of standards. For details of these and other benefits contact Membership Administration. Tel: +44 (0)20 8996 7002. Fax: +44 (0)20 8996 7001. Email: membership@bsi-global.com.

Information regarding online access to British Standards via British Standards Online can be found at <http://www.bsi-global.com/bsonline>.

Further information about BSI is available on the BSI website at <http://www.bsi-global.com>.

Copyright

Copyright subsists in all BSI publications. BSI also holds the copyright, in the UK, of the publications of the international standardization bodies. Except as permitted under the Copyright, Designs and Patents Act 1988 no extract may be reproduced, stored in a retrieval system or transmitted in any form or by any means – electronic, photocopying, recording or otherwise – without prior written permission from BSI.

This does not preclude the free use, in the course of implementing the standard, of necessary details such as symbols, and size, type or grade designations. If these details are to be used for any other purpose than implementation then the prior written permission of BSI must be obtained.

Details and advice can be obtained from the Copyright & Licensing Manager. Tel: +44 (0)20 8996 7070. Fax: +44 (0)20 8996 7553. Email: copyright@bsi-global.com.