BRITISH STANDARD

BS 15000:2000

Specification for

IT service management

ICS 35.020

NO COPYING WITHOUT BSI PERMISSION EXCEPT AS PERMITTED BY COPYRIGHT LAW

Information Handling Services, 2000

STD.BSI BS 15000-ENGL 2000 ■ 1624669 0881040 0T2 ■

Committees responsible for this British Standard

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

British Computer Society (BCS)
Central Computer and Telecommunications Agency (CCTA)
IT Service Management Forum (itSMF)
National Audit Office (NAO)
Co-opted members

This British Standard, having been prepared under the direction of the DISC Board, was published under the authority of the Standards Committee and comes into effect on 15 November 2000

© BSI 11-2000

Amendments issued since publication

Amd. No.	Date	Comments

The following BSI references relate to the work on this standard:
Committee reference BDD/3
Draft for comment 00/683007 DC

ISBN 0 580 33233 0

Information Handling Services, 2000

Contents

Information Handling Services, 2000

Foreword

This British Standard has been prepared by Technical Committee BDD/ 3. It is based on, and may be used in conjunction with, DISC PD 0005, *A Code of Practice for IT Service Management*, which provides guidance on best practice and supports the requirements of this standard. This standard may also be used in conjunction with DISC PD 0015, *IT Service Management — Self-assessment Workbook*, which contains a number of checklists designed to assist organizations assess the extent to which their IT services conform to the requirements of this standard.

The list of control objectives and controls contained in this standard is not exhaustive and an organization may consider that additional control objectives and controls are necessary to meet their particular business needs.

The nature of the business relationship between the service provider and customer will determine how the requirements in this standard are implemented in order to meet the overall objective.

The organization, or department within an organization, that is being assessed for compliance is required, as part of the process, to define their "boundary" of activities to be certified. The boundary needs to be approved by the auditor and, assuming certification is granted, appears on their certificate of compliance. Any organization seeking to rely on a service provider's claimed compliance with the standard should first ask to see their certificate so that they can check what is included within it.

To summarize, the organization applying for certification has to comply with all the specified processes, but, by defining their boundary of certification, may choose to include or exclude customer or supplier activities as they wish.

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 the necessary provisions of a contract. Users of British Standards are responsible for their correct application.

Compliance with a British Standard does not of itself confer immunity from legal obligations. Attention is drawn to the following legislation:

Data Protection Act 1998.

Computer Misuse Act 1995.

Copyright, Designs and Patent Act 1988.

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.
Shirley Lacy	Change IT Ltd. and representative of the BCS
Don Page	Marval Software Ltd.
Ivor Macfarlane	Guillemot Rock
Lynda Cooper	F.I. Group plc
Ivor Evans	Ivory Consulting Ltd.
Aidan Lawes	itSMF
Martin Carr	CCTA
John Groom	CCTA
Ian Petticrew	NAO

The Committee also wishes to acknowledge the support of the British Broadcasting Corporation as sponsors of this standard.

Summary of pages

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

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

© BSI 11-2000

Information Handling Services, 2000

1 Scope

This standard specifies service management processes and forms a basis for the assessment of a managed IT service. It may be used by:

— organizations seeking tenders for outsourced services;

— organizations that require a consistent approach by all service providers in a supply chain;

— existing providers to benchmark their IT service management;

— as the basis for formal certification.

The relationship between different service design and management processes is illustrated in Figure 1.

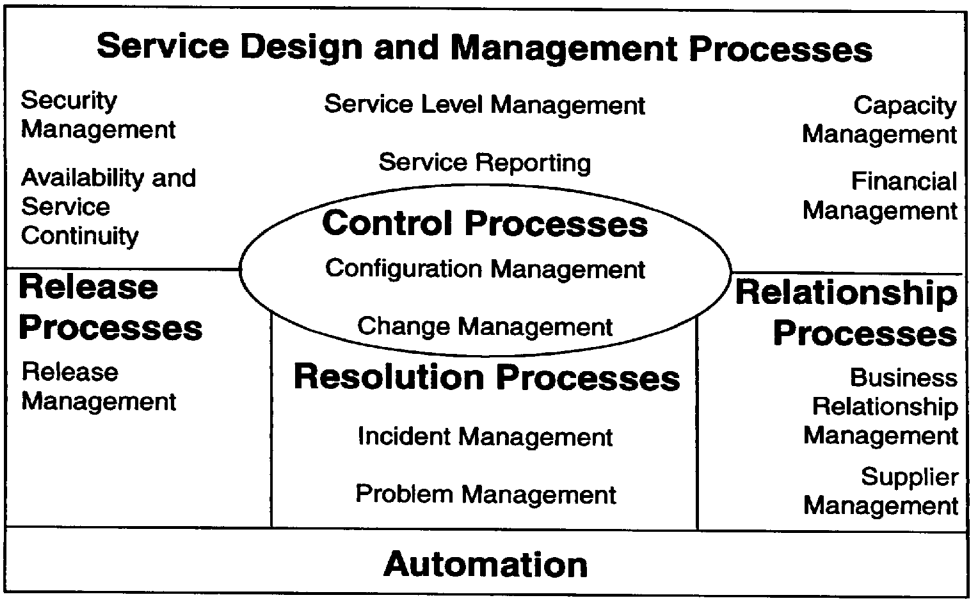

Figure 1 — Service design and management processes

2 Normative reference

The following normative document contains provisions which, through reference in this text, constitute provisions of this British Standard. The latest edition of this publication applies.

DISC PD 0005, *Code of Practice for IT Service Management.*

3 Definitions

For the purposes of this British Standard, the definitions given in DISC PD 0005, excepting the following, apply.

3.1

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 customers to the agreed service hours.

3.2

change management

process of managing changes to the infrastructure or any aspect of services in a controlled manner, allowing approved changes to be made with minimum disruption

© BSI 11-2000

Information Handling Services, 2000

3.3

change record

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

3.4

charging

process of establishing charges in respect of business units and raising invoices

3.5

classification

process of formally identifying incidents, problems and known errors by relevant categories such as origin, symptoms and cause

NOTE This is principally an internal process aimed at aiding root cause analysis.

3.6 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.

3.7

configuration management

process of identifying and defining the configuration items in a system, recording and reporting the status of configuration items and verifying the completeness and correctness of configuration items

3.8

cost

actual or notional amount of expenditure incurred on, or attributable to, a specific service or business unit

3.9

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.

3.10

impact

measure of the scale and magnitude of an incident, problem or request for change

3.11

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.

3.12

knowledge base

repository containing data relevant to the execution of any of the service management processes and available to appropriate staff where and when required

3.13

known error

incident or problem for which the root cause is known

NOTE All but this definition are identical to those definitions also used in ITIL®[1]. ITIL®[1] offers a more detailed perspective and takes the definition a stage further to include the resolution (temporary or otherwise) of the error.

3.14

metric

measurable element of a service process or function

[1] ITIL® is a registered trade mark of the Central Computer and Telecommunications Agency (CCTA).

Information Handling Services, 2000

3.15

problem

unknown underlying cause of one or more incidents

3.16

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.

3.17

release

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

3.18

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

3.19

service improvement programme

series of activities undertaken within an enterprise to identify and introduce measurable improvements within a specified service or work process

3.20

service level agreement (SLA)

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

3.21

service level management

process of defining, agreeing, implementing and managing the levels of customer service

3.22

service management

management of services to meet the customer's requirements

3.23

system

integrated composite that consists of one or more of the processes, hardware, software, facilities and people that provides a capability to satisfy a stated need or objective

3.24

third-party supplier

enterprises or groups, external to a service supplier's enterprise, which provide services and/or products that contribute to, or supplement, the overall service

3.25

workaround

method of avoiding the impact of an incident or problem, either from a temporary fix or from a technique that means the customer is not reliant on a particular aspect of the service that is known to have a problem

Information Handling Services, 2000

4 General

4.1 Establishing the boundaries of the managed service

Objective: To define the boundary of the managed service.

The scope of the managed IT service shall be defined. The boundaries shall be defined in terms of the characteristics of the organization, its location, assets and technology.

4.2 Service management planning

Objective: To provide management direction and resources for implementing service management activities.

A service management plan shall define:

a) the scope of service management within the organization;

b) the objectives that are to be achieved;

c) the framework of management roles and responsibilities, including the management of third-party suppliers;

d) the interfaces between service management activities and the manner in which activities are to be coordinated;

e) the approach to be taken in identifying, assessing and managing risks so the defined objectives are achieved;

f) the resources necessary to achieve the defined objectives.

A service management plan shall include information concerning its implementation, maintenance and authorization. A cross-functional management forum shall provide support for prioritizing, planning and coordinating service management activities. Customers and third-party suppliers shall appoint individuals to act as points of contact for their organizations.

Procedures that are developed for compliance with this standard shall also support the objectives of the service management plan and shall be auditable.

4.3 Professional competence

Objective: To ensure that service management personnel are competent.

Service management roles and the competencies necessary to discharge them effectively shall be defined.

Service management personnel who are permanent employees of the service provider shall receive structured education and training in service management appropriate to their role(s). A record shall be maintained for each individual of training received and current competencies. Individuals' development needs shall be reviewed at least annually with the aim of maintaining competencies and developing them where appropriate.

Service management personnel who are not permanent employees of the service provider shall be required by the service provider to furnish documentary evidence of their qualifications, skills and experience and to maintain the relevant competencies.

NOTE This may include agency personnel, contractors and consultants.

Responsibility shall be assigned for managing these requirements.

4.4 Service quality

Objective: To demonstrate evidence of continual improvement in the quality of the service.

There shall be an ongoing programme of activities designed to monitor and improve the quality of the service. Metrics and targets shall be defined for each service management process and used as a basis for monitoring service quality. Formal methods shall be adopted that permit meaningful comparisons in service quality to be made, including the comparison of actual achievements with corresponding targets over different reporting periods. A history of service level targets and results shall be maintained together with any actions designed to improve the service.

Information Handling Services, 2000

A report on the outcome of service quality monitoring shall be published at least annually and made available to customers. The report shall identify:

a) service management targets and the corresponding results achieved for the current reporting period;

b) for purposes of comparison, service management targets and the corresponding results achieved for the previous reporting period;

c) the objectives of improvement actions that are to be undertaken during the forthcoming reporting period.

4.5 Audit evidence

Objective: To provide evidence of service management operations.

All service management policies and plans shall be documented.

Procedures and responsibilities shall be established for the creation and maintenance of documents that shall be:

a) readily identifiable and available;

b) dated, and authorized by a designated person;

c) legible and readable;

d) maintained under version control and available to all locations where service management activities are performed;

e) promptly withdrawn when obsolete and retained in/as an archive where required for legal or knowledge preservation purposes, or both.

Records shall be:

1) readily identifiable and available;

2) dated and authorized in accordance with relevant procedures;

3) legible and readable;

4) protected against damage, deterioration or loss;

5) retained for a period sufficient to meet the requirements of this specification;

NOTE Other business requirements may demand longer retention periods.

6) disposed of securely when no longer required.

4.6 Demonstrating conformity

Objective: To demonstrate implementation of the service management objectives.

The service management objectives shall be audited against this standard at least annually. Audits shall be undertaken by competent personnel who were not involved in the development or implementation of the service to be audited and are not involved in its operation or maintenance.

In addition to these independent audits, managers shall regularly review the operation of service management activities within their area of responsibility to monitor conformity with service management policies and procedures.

5 Service design and management

5.1 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, shall be agreed by the parties and recorded. SLAs, together with underpinning operational service level objectives, third-party contracts and corresponding procedures, shall be agreed by all parties and recorded.

The SLAs shall be maintained by regular reviews by all parties to ensure that they are up-to-date and effective. SLAs shall be subject to change management, as specified in **8.2**.

Reasons for non-conformity to service levels shall be documented and reviewed and shall be fed into the service improvement programme.

5.2 Availability management

Objective: Availability management is to be used to translate and integrate requirements contained in SLAs into availability targets.

Availability shall be defined, measured, recorded and delivered in terms of the services required for the business processes and access to those services.

The SLA requirements shall be used to plan availability.

Actual performance against availability targets shall be monitored regularly. The results of monitoring shall be fed into the service improvement programme. Details of any corrective actions shall be recorded.

Information Handling Services, 2000

5.3 Service continuity

Objective: To ensure that agreed obligations to customers can be met in the event of service failure or disaster.

Service continuity requirements shall be identified on the basis of the customer's business priorities. Formal plans and support contracts shall be developed to ensure that these requirements are met in the event of prolonged service failures and disasters that impact the service provider and/or the customer(s) and/or relevant third parties.

NOTE 1 Service failures and disasters may be outside the supplier's control, for example, failures of public infrastructure, natural disasters.

Service continuity plans shall be kept up-to-date to ensure that they reflect the changing manner in which services are delivered to customers and changing customer requirements.

NOTE 2 The service provider's conditions of business should encourage customers to test their service continuity plans at least annually to ensure that they are workable and continue to meet the customer's business needs. This can be done by making reasonable time and resources, including expert advice, available to the customer.

5.4 Service reporting

Objective: To produce timely, reliable, concise and meaningful reports for decision support.

There shall be a clear description of the identity and purpose of each service report and of the data from which each report is derived.

Service reports shall be produced to meet the needs of all decision makers.

NOTE For example, the service report may contain:

a) service level monitoring and reporting;

b) problem and change management;

c) configuration management;

d) financial reporting.

5.5 Financial management

Objective: To control and account for the cost of service provision and its recovery, where applicable.

There shall be clear policies and procedures that define how services should be authorized, budgeted, charged and accounted for.

Costs shall be forecast in an annual budget in sufficient detail to enable effective financial control and decision making. The service provider shall monitor forecasts against the corresponding costs incurred during each financial control period and record actions that are taken.

Any agreement between the service provider and customer on the reporting of financial information, including its frequency and format, shall be recorded in the corresponding SLA. Changes to services shall be costed and approved before development work commences.

5.6 Capacity management

Objective: To ensure the organization has, at all times, sufficient resources to deliver the business workload.

Methods and procedures shall be defined for monitoring service capacity and tuning system performance.

Capacity management planning shall include:

a) capacity predictions and agreed response times;

b) agreement on time-scales or thresholds for service upgrades, e.g. upgrade when the number of users reaches a predefined threshold;

c) an evaluation of the effects of anticipated service upgrades, new technologies and techniques;

d) predictions of the impact of external changes, e.g. more users, legislative;

e) procedures, tools and methods to achieve and monitor the service capacity;

f) the data and processes to enable predictive trend analysis.

5.7 Information security management

Objective: Effective management of information security within service management activities.

NOTE 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.

Information Handling Services, 2000

Management with executive responsibility shall approve an information security policy that shall be published and communicated to service management personnel and customers.

A management organization shall maintain the information security policy, coordinate its implementation and provide specialist advice on information security risk assessment and the implementation of controls.

Controls shall operate to:

a) implement the requirements of the information security policy;

b) manage risks associated with third-party access to the service or systems;

c) meet the security requirements that are agreed with customers.

Controls shall be documented to describe the risks to which they relate and their manner of operation and maintenance. 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 or contract that defines all necessary security requirements.

Security incidents shall be reported through management channels to agreed contacts as soon after an incident is discovered as possible. All security incidents shall be recorded, investigated and management action taken. The types, volumes and costs of security incidents and malfunctions shall be quantified and monitored and the results shall be fed into the service improvement programme.

6 Relationship processes

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

6.1 Business relationship management

The service provider and customer shall conduct a joint performance review against the SLA and business needs at least annually and shall hold interim meetings at agreed intervals to discuss progress, achievements, issues and future plans.

Actions identified during service reviews shall be recorded and introduced into the service improvement programme.

All service complaints shall be recorded, investigated, acted upon and formally closed. Where a complaint cannot be resolved through the normal channels, a separate procedure, with the involvement of more senior management, shall be available to the customer.

A process shall exist for obtaining and acting upon feedback from regular customer satisfaction measurements.

6.2 Supplier management

Objective: To ensure a seamless, quality provision of service from the party supplier.

Contracts and agreements with suppliers shall be reviewed:

a) to ensure that the services provided continue to meet business needs;

b) when significant changes to service requirements take place;

c) at least annually.

Procedures shall be in place:

1) for monitoring the performance of service suppliers;

2) for performing service reviews at agreed intervals, and at least annually;

3) for progress, achievements, issues and future plans to be discussed;

4) to cover contractual disputes;

5) for the amendment of the contract and level of service in the event of changes.

The scope, level of service and interface processes to be provided by the supplier shall be documented and agreed by both parties.

Services provided by lead suppliers shall demonstrate processes to ensure that subcontracted suppliers meet contractual requirements.

Information Handling Services, 2000

STD.BSI BS 15000-ENGL 2000 ■ 1624669 0881050 T41 ■

7 Resolution processes

7.1 Incident management

Objective: To reduce service degradation by managing incidents throughout their complete lifecycle.

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

The customer shall be kept informed of the progress of their reported incident at predetermined intervals and informed if agreed service levels cannot be met.

All staff involved in incident management shall have access to the knowledge base.

7.2 Problem management

Objective: To identify and manage the underlying causes of service incidents whilst minimizing or preventing disruption to customers.

Incident records shall be analysed regularly to detect frequently occurring incidents and trends. The results and conclusions drawn from analyses of those records shall be recorded. Potential problems shall be identified to prevent their occurrence.

Procedures shall be adopted to identify, minimize or avoid the impact of service problems. They shall define the recording, prioritization, classification, updating, escalation, resolution and closure of all problems within agreed time-scales.

Corrected problem areas shall be monitored, reviewed and reported on for effectiveness.

All staff involved in problem management shall be responsible for ensuring problem information and related information is available and up-to-date.

All identified known errors, workarounds and solutions shall be added to the knowledge base.

8 Control processes

8.1 Configuration management

Objective: To account for and control the components of the service or infrastructure and protect the integrity of the information systems and environments.

NOTE Financial asset accounting falls outside the scope of this standard.

Planning for change, configuration and release management shall address:

a) the definition of configuration items;

b) the scope and objectives of change and configuration management;

c) the integration of change, configuration and release management activities;

d) organizations, roles and responsibilities of the parties involved in controlling the configurations, changes and releases;

e) procedures for identification, configuration change and release control, status accounting, configuration verification and auditing of configuration items.

All configuration items shall be uniquely identifiable and recorded in an inventory to which update access shall be strictly controlled. The inventory shall be actively managed and verified at scheduled intervals to ensure its reliability. The status of changes to assets and configuration items, their versions and associated documentation shall be visible to all relevant parties.

Changes to configuration items and movements of software and hardware shall be managed, traceable and auditable. Configuration control procedures shall ensure that the integrity of systems, services and data are maintained and protected from corruption.

Master copies of software, testing products and documents shall be controlled in secure physical or electronic libraries and referenced to the configuration records.

Configuration audit procedures shall include the method of recording deficiencies, assessing risks, reporting the outcome and instigating corrective actions. Corrective actions shall be recorded, acted upon and fed back to the service manager and the service improvement programme.

Software licence structures, corporate and multi-licensing schemes shall be documented clearly and communicated to appropriate staff and customers.

© BSI 11-2000

Information Handling Services, 2000

8.2 Change management

Objective: To ensure that changes to the business requirements, infrastructure or services are assessed, approved and implemented in a controlled manner.

Procedures shall be adopted to ensure that changes to the infrastructure and services are implemented in a controlled manner. They shall specify the manner in which business, infrastructure and service changes shall be:

a) assessed for their impact and risk on the service, business, customer, infrastructure and release plans;

b) inspected and tested to ensure acceptable quality;

c) authorized for implementation;

d) linked to associated incident, problem, other change and configuration item records;

e) remedied if there are problems during implementation.

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

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 and acted upon.

There shall be formal procedures to control the implementation of emergency changes. All emergency changes shall be recorded in sufficient detail to enable management reviews. Where emergency procedures permit a change to bypass other change management requirements, the change shall conform to these requirements as soon as is practicable.

Policy and procedures shall be defined for undertaking post-implementation reviews of major changes. These shall require that:

1) any unsatisfactory aspects of a change (for example, with regards to its actual cost, usability and functionality compared with what was planned) are recorded;

2) any weaknesses or deficiencies in the change control process are recorded.

8.3 Implementation of new or changed service

Objective: To plan the implementation of new or changed services and demonstrate the outcomes achieved.

The implementation of new or changed services shall be planned and approved through the change management process (see **8.2**). Plans shall identify:

a) the roles and responsibilities for implementing, operating and maintaining the new service, including activities to be performed by customers and third-party suppliers;

b) changes to the existing service management framework;

c) manpower and recruitment requirements;

d) skills and training requirements;

e) the methods and tools to be used in connection with the new or changed service;

f) budgets and time-scales;

g) the expected outcomes from operating the new service expressed in measurable terms.

The service provider shall report on the outcomes achieved by the new service against those planned as soon as practicable following its implementation. The report shall be made available to relevant customers and the results shall be fed into the service improvement programme, if appropriate.

9 Release management

Objective: To plan the content and roll-out of a release to ensure that any configuration items changed are correct, traceable, secure and authorized.

The service provider shall plan the release of software and hardware. Plans shall record the release dates, deliverables and refer to related changes, known errors and problems.

Plans on how to roll-out the release to each location and user shall be agreed and signed off by all relevant parties.

Information Handling Services, 2000

Software libraries and related repositories shall be used for managing and controlling software during the release process. Software release and distribution should be designed and implemented so that the integrity of hardware and software is maintained during installation, handling, packaging and delivery. Procedures shall be adopted to:

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

b) verify that a software release is complete when it reaches its destination;

c) ensure that only suitably tested hardware and software are accepted and released into operational use;

NOTE Authorization will be performed through the change management process.

d) decommission redundant products, services and licences.

The number of incidents in the period immediately following a release shall be measured and analysed to assess their impact on the business, IT operations and support staff resources. Recommendations shall be fed into the service improvement programme.

Information Handling Services, 2000

Annex A (informative)

Other sources of information

Further details of the subjects covered in this standard are available in the publications within ITIL®[2].

British Computer Society[3]

British Computer Society: www.bcs.org.uk
British Computer Society Configuration Management Group: www.cmsg.org.uk

IT Service Management Forum (itSMF)

itSMF: www.itsmf.com

[2] ITIL® is a registered trade mark of the Central Computer and Telecommunications Agency (CCTA). ITIL® is developed through an open and collaborative process involving user and vendor organizations worldwide. Further details can be found on www.itil.co.uk. ITIL® publications are available from The Stationery Office, 123 Kingsway, London WC2B 6PQ Tel: 020 7242 6393, BSI Customer Services, 389 Chiswick High Road, London W4 4AL Tel: 020 8996 9001 or from itSMF.

[3] Further details are available from the British Computer Society, 1 Sandford Street, Swindon SN1 1HJ Tel: 01793 417417.

Information Handling Services, 2000

Bibliography

BS 7799-1:1999, *Information security management — Part 1: Code of practice for information security management.*

BS 7799-2:1999, *Information security management — Part 2: Specification for information security management systems.*

Information Handling Services, 2000

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: 020 8996 9000. Fax: 020 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: 020 8996 9001. Fax: 020 8996 7001.

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: 020 8996 7111. Fax: 020 8996 7048.

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: 020 8996 7002. Fax: 020 8996 7001.

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.

If permission is granted, the terms may include royalty payments or a licensing agreement. Details and advice can be obtained from the Copyright Manager. Tel: 020 8996 7070.

BSI
389 Chiswick High Road
London
W4 4AL

Information Handling Services, 2000