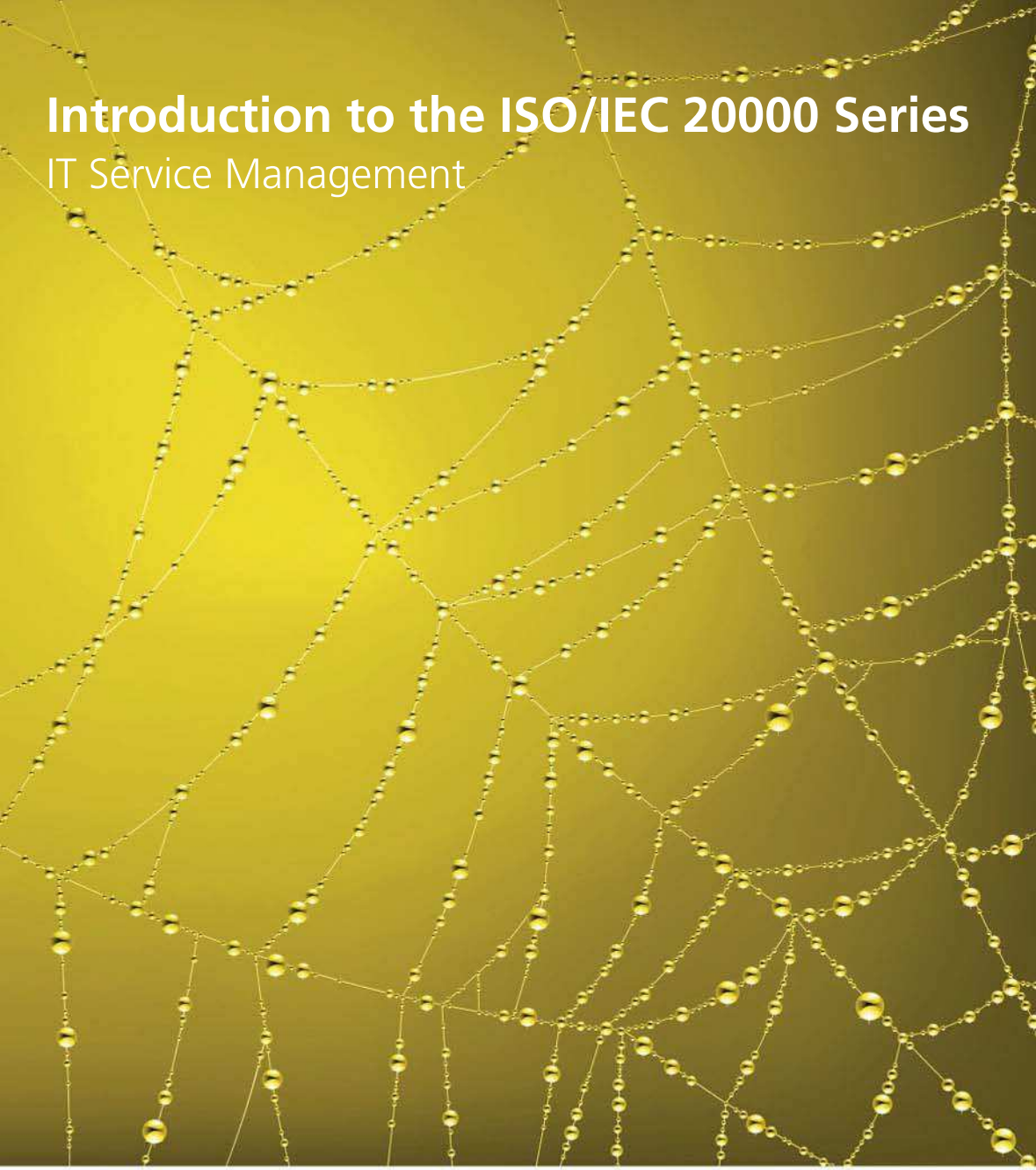
Introduction to the ISO/IEC 20000 Series

IT Service Management



Jenny Dugmore and Shirley Lacy

BSI

Introduction to the ISO/IEC 20000 Series

IT Service Management

Introduction to the ISO/IEC 20000 Series

IT Service Management

Jenny Dugmore and Shirley Lacy

First published in the UK in 2011
by
BSI
389 Chiswick High Road
London W4 4AL

Typeset in Frutiger by Letterpart Limited, www.letterpart.com
Printed in Great Britain by Berforts Group, www.berforts.co.uk

British Library Cataloguing in Publication Data
A catalogue record for this book is available from the British Library

ISBN 978-0-580-72846-4

Contents

Acknowledgements

This book has been produced with the input and assistance of people involved in the practical aspects of delivering services across all sectors and many of those actively involved in the development of the 20000 series. We would like to thank them for sharing their views and providing constructive criticism, examples and practical techniques.

We wish to thank the technical experts for all the energy, effort and excellent input given to the production of the 20000 series. It's been an interesting journey for us all and we have collectively moved the 20000 series on a long way.

We also wish to thank the individuals who have reviewed the book and contributed ideas and practical experience:

Diego Berea Cabaleiro
David Cannon
Erin Casteel
Jim Clinch
Lynda Cooper
Nick Fright
Steve Ingall
Bridget Kenyon
Greg Lake
Michelle Hales
Alastair Walker
Jack Robertson-Worsfold
Sharon Taylor

Finally, we would like to thank Julia Helmsley and Siobhán FitzGerald of BSI for their support, helpful suggestions, tact and patience during the production of this book.

Foreword

Organizations are more dependent on IT services than ever and face the challenge of constant business and technology change. Many are concerned whether their IT services align with the needs of the business and its customers.

ISO/IEC 20000 is an internationally recognized set of standards for IT service management that is used around the world. There are many reasons for an organization to use the 20000 series and to implement the requirements specified in Part 1. For example, a service provider certified under Part 1 has independent proof of having implemented best practices, such as those in the ITIL®[1] IT Service Management framework.

Certification to ISO/IEC 20000-1 by an accredited certification body shows that a service provider is committed to delivering value to customers and continual service improvement. It demonstrates the existence of an effective service management system that satisfies the requirements of an independent external audit. Certification gives a service provider a competitive edge in marketing.

A service management system also provides support for corporate governance. For example, disclosure and financial reporting are important aspects of corporate governance. These are reliant on information from and the support of the processes in the 20000 series. Governance integrates and institutionalizes good practices for planning and organizing, acquiring and implementing, delivering and supporting, and monitoring the performance of services. This approach helps to ensure that an organization's information and related technology supports its business objectives. Governance enables an organization to take full advantage of its information, maximizing benefits, capitalizing on opportunities and gaining competitive advantage.

The 20000 series is driven by the continual improvement of processes and services, so a service provider will normally find that implementing the requirements in Part 1 gives an improved service that adds much greater value to the customer. In turn this enables the customers to be more effective.

[1] **ITIL® is a Registered Trade Mark of the Office of Government Commerce in the United Kingdom and other countries**

Implementing best practice service management can reduce costs at the same time as the quality of the service improves. Customer satisfaction improves and the number and seriousness of complaints is reduced. This can lead to a reduced management overhead of resolving complaints and dealing with unhappy users. Managers are set free to proactively manage services and change.

Introduction

Service management

Service management is defined as a set of capabilities to direct and control a service provider's activities and resources to deliver and improve services. A service provider applies these capabilities to the design, transition, delivery and improvement of services, to fulfil service requirements.

Target audience

The 20000 multi-part series is applicable to many organizations, both internal and external service providers, public and private sector, large and small. Part 1 of the series is ISO/IEC 20000-1, requirements for a service management system.

This book will help those that are interested in:

- certification under Part 1;
- performing either certification or internal audits using Part 1 requirements;
- service and process improvement using the 20000 series;
- best practice service management, such as ITIL®;
- becoming personally qualified in service management;
- assurance that their service requirements will be fulfilled with a greater consistency in approach across their service supply chain.

This book will also be of interest to customers and business managers who interact with service providers as part of their responsibilities.

This book covers the 20000 series, including all aspects of the ISO/IEC 20000-1 requirements for IT service management, based on the second edition of Part 1, published in 2011.

This book covers requirements and advice for a range of service management processes using figures, tables, checklists and examples. It uses material from the 20000 series. The chapters are:

Chapter 1 explains the whole 20000 series and the way the other parts can be used to help achieve the requirements in ISO/IEC 20000-1:2011.

Chapter 2 describes the approach to defining the scope of a service management system (SMS).

Chapters 3 to 5 cover the establishment of an SMS that fulfils the requirements of ISO/IEC 20000-1, including the approach to integrating processes.

Chapter 6 covers the importance of people in delivering services. Personnel need to be well organized and co-ordinated. This chapter provides advice on some aspects of managing and motivating managers and personnel.

Chapter 7 includes advice on the correct process for control of documentation and what can be required as part of evidence for a certification audit.

Chapters 8 to 13 cover service reporting and the management of the service supply chain provided by supplier management, service level management (SLM) and business relationship management (BRM). It describes aspects of information security, managing capacity, service continuity and availability and financial issues.

Chapters 14 to 17 cover the resolution processes and the closely related control processes: configuration, change and release and deployment management.

Chapter 18 explains the requirements for the design and transition of new and changed services including the interaction with the control processes. It includes advice on the issues that are likely to be encountered when major changes are implemented and the way these should be avoided or managed.

Annexes include the terms used in the 20000 series (Annex A). Annex B includes the content lists from each part of the 20000 series. Annex C includes the documents and records that can be required as evidence during an audit. Annex D is a case study and the final annex is a Bibliography.

Chapter 1 20000 is now a series

Introduction

The first editions of the International Standards ISO/IEC 20000-1 and ISO/IEC 20000-2, referred to as Parts 1 and 2, were published in 2005. This followed a fast-track process of a two part UK standard BS 15000.

The second edition of Part 1 is now available with the second edition of Part 2 due soon.

The parts of the 20000 series already published include Parts 3, 4 and 5. These are currently Technical Reports providing guidance on service management. Each document in the series supplements and complements the others. The published and planned parts of the series are described below.

The five published parts of the 20000 series are summarized in the table below.

Table 1 – The published 20000 series

Part	Status	Title/scope
1	International Standard, 2011	Requirements for a service management system
2	International Standard, due soon	Guidance on the application of service management systems
3	Technical Report, 2009	Guidance on the scoping and applicability of ISO/IEC 20000-1
4	Technical Report, 2010	Process reference model for IT service management
5	Technical Report, 2010	An exemplar implementation plan for ISO/IEC 20000-1

To what does 20000 apply?

The multi-part 20000 series is applicable to many organizations, both internal and external service providers, public and private sector. The 20000 series applies equally to an internal service provider funded as an operating overhead and to one 'charging' via transfers between internal

cost-codes. It applies to a commercial organization providing outsourced services to large organizations and to service providers delivering Internet-based services to individual customers paying a monthly subscription.

The 20000 series is applicable to service providers of all sizes ranging from less than 10 people to many hundreds of thousands of personnel. While the requirements remain unchanged for large or small organizations, the ways those requirements are fulfilled may differ significantly. For example, a large service provider would need sophisticated capacity management planning; a small organization would meet Part 1 requirements and function effectively with a very basic plan.

The series is useful for an organization subject to regulations or legislation covering their activities, such as the finance or the pharmaceutical sectors.

The 20000 series is also applicable to service providers who rely on some services delivered by other parties. The series is independent of organizational structure or the technologies used for the delivery of services or to automate service management. Technology does not change the requirements in Part 1, but can have an impact on the skills, tools and data needs.

Annex D contains a case study for a service provider who gained benefits from being certified under edition 1 of ISO/IEC 20000-1, published in 2005.

The service provider's CEO said:

> *We are now more focused on delivering end-to-end services that create value for our business and our external customers. Investing in developing our service management capability has enabled business transformation whilst maintaining control. Achieving certification to ISO/IEC 20000-1 is good marketing for delivering world class IT services and we are growing our customer base.*

This service provider is planning on converting to certification under edition 2 of ISO/IEC 20000-1, published in 2011.

The 20000 series

Part 1

Part 1 is the core of the 20000 series and is the basis for establishing a service management system (SMS), continual service improvements, management reviews, internal and certification audits. Part 1 requirements are compulsory for a certification audit.

The differences between the first and second editions of Part 1 have been summarized in the table below.

Table 2 – The key differences between Part 1 editions 1 and 2

The most important changes are linked to the reality faced by many service providers: how the contribution made by other groups to the overall service should be managed.
The first step was the publication of Part 3, on the scope of the service management system, services and service management. Part 1 now includes a new Clause 4.2 on the governance of processes. This is a short but exacting clause on how the contribution should be managed and what the service provider has to do to be in control of the overall service.
The new requirements cover additional control for suppliers, internal groups and customers acting as suppliers. Part 1 uses the term internal groups for in-house suppliers not under the direct control of the service provider. Customers acting as suppliers are groups that contribute part of the overall service. As part of the customer's organization they are not managed directly by the service provider.
The requirements for process governance are linked to the new requirements in Part 1 for defining scope, when it should be done and what parameters are required. Scope is affected by what suppliers and other parties contribute, so clarity on this is more important than ever before. Scope is also affected by the services, customers, types of hardware and locations.
The new edition of Part 1 has several important features to support its international use.
Wording has been standardized so that it translates more easily and consistently. For example, Part 1 does not now use 'management control', because of difficulties in translation. Instead Part 1 uses just 'management' or 'control' or 'governance of processes', depending on the context.
There are more special terms included. When possible Part 1 uses the same special terms as ISO 9001 and ISO/IEC 27001. Service management terms have been extended, but Part 1 still relies mainly on words being used with the meanings in commonly used dictionaries.
There are some structural changes, for example Clauses 3 and 4 have been merged to give a larger Clause 4, general requirements for a service management system, including more requirements for continual improvement.
Part 1 is longer. New requirements include a service catalogue, when previously this was only a recommendation. Other changes include the introduction of requirements for service request management and release becoming release and deployment.

Other changes include new requirements for services that are considered to be at higher than usual risk from changes. The new and changed service process in Clause 5 now includes the first stage of the service lifecycle, both planning and design of services, so that the service provider is aware of new services soon enough to avoid any bad decisions made early in planning and design.

Some named roles, such as process owner, are not now used in Part 1, but the role and responsibilities are still included.

ISO is completely independent of certification or qualification schemes and does not say how the changes will impact schemes or how long the changeover should take. There will be a phased changeover defined and managed by the owners of each scheme, of which there are now several world-wide. The changeover may differ across schemes so clarification should be sought from scheme owners.

The two editions of Part 1 are compared in detail in *A Guide to the New ISO/IEC 20000-1: The differences between the 2005 and 2011 editions*.

Part 2

The second edition of Part 2 is close to completion. It provides guidance on the application of an SMS, describing the intent, concepts and requirements for each process in Part 1. It provides advice on the roles and responsibilities and the documents and records required.

Part 3

Part 3 includes advice on evidence that will be required during an audit against Part 1 requirements. However, its most significant contribution to the 20000 series is guidance on defining the scope of an SMS. As a result of this, Part 3 also provides advice on how to define the scope of service management.

Part 3 explains when Part 1 is applicable. For example, does the service provider have governance of all processes, including any processes operated by other parties? Can the service provider agree an acceptable scope statement for a certification audit? To provide additional help, examples of the reverse are also included, i.e. where Part 1 may not be used for a certification audit.

Part 3 is underpinned by practical, scenario-based guidance, illustrating the way the 20000 series may be used by a service provider faced with a range of the most common circumstances.

Part 1 requires the service provider to demonstrate governance of any processes operated by other parties. Failure to show that a service provider is in control will mean that the scope will be restricted and the service provider might not be able to fulfil all Part 1 requirements. As a direct consequence, Part 3 is essential reading for any service provider that has asked another organization to manage their services or operate any of their service management processes.

Part 4

Part 4 is a service management process reference model, aligned to Part 1. The process reference model defines each Part 1 process using inputs, outputs and activities. Although it can assist with process design it was developed as the basis of a five-level assessment model, which is under development.

Part 5

Part 5, published in 2010, includes practical '*what to do when*' advice for a three phase implementation of an SMS. Such a phased implementation incurs lower risks and costs than doing everything in a single step. It includes practical examples and is partly based on scenarios that apply to most service providers.

In Part 5, the first phase is the implementation of those parts of the SMS that support the quick and effective reaction to service disruptions. For example, Phase 1 includes most of incident management but only basic service reporting.

More is implemented in Phase 2: the service provider is then able to anticipate service disruptions or requests and to provide a more reliable service. For example, the more advanced or proactive aspects of processes established in Phase 1 or processes such as release management that require a more mature approach to service management.

Phase 3 involves integration and consolidation of all processes, improvements in established processes and procedures. It also includes implementation of the design and transition of new or changed services, which interfaces to major or higher risk projects. The end result of Phase 3 is an SMS that conforms to Part 1, with consolidation and continual improvement carried on afterwards.

Service providers with an incomplete SMS can use Phase 1 as a programme of improvements to what is already in place. Part 5 is generic, so can be used by most service providers.

What about Parts 6 onwards?

Other parts are being considered, with a focus on explaining the way the requirements in Part 1 map and align to other standards, methods and frameworks. These proposals were identified by market research.

Market research continues to play a part in identifying what will (or will not) be developed in support of Part 1.

The style guide used to keep the 20000 series consistent is being incorporated in a new Part 10, with the title 'Concepts and terminology'. It will contain the special terms used in the 20000 series.

Terminology

In Part 1, each requirement is indicated by the use of 'shall'. The verb 'shall' is not used in the rest of the 20000 series, which contains advice and not requirements.

In Part 1 and the rest of the 20000 series the verb 'may' is used to show something is permitted under the Part 1 requirements, but is not compulsory. The verb 'can' is used if something is possible, but again it is not compulsory.

Part 1 includes a few notes. These are not part of the requirements and will not be used in an audit. They are primarily used to provide supporting information that is intended to help the user understand and apply the requirements. An example is the note in Part 1, Clause 1.2 that refers to Part 3 as a useful source of information on scope definition and applicability.

Part 1 does not require a service provider to use the terms used in the 20000 series, although there should be no ambiguity about what each process includes. It is usually easier for a service provider to adopt common industry terms. If this has not been done, an auditor will find it useful to have a mapping of the service provider's terms with those used in the 20000 series. This is particularly important for the special terms, in Part 1, Clause 3, which are also included in Annex A.

Key point

> Special terms are included in Part 1, Clause 3. All other terms are 'normal' words, with the meaning given in widely used UK English language dictionaries. The consistent use of 'normal' words has helped with understanding, interpretation and translation. It has helped keep the 20000 series aligned. Jargon is not allowed, so for example, a scope is defined because 'scoping' is not in dictionaries, although 'scoping' is often used in conversations.

The consistency of usage will add value for native English speakers, but most of the benefit will be for readers from the many different language groups that now use the 20000 series.

Consistency of usage supports consistency of translation into other languages, in particular for words with no exact equivalent in the target language.

English is a flexible, context sensitive and evolving language, where a word can mean something different according to the context in which it is being used. However, this use of standardized, normal UK English has also been codified as a style guide to keep the wording in each part and across the whole 20000 series consistent.

Examples include 'establish' to mean *'to set up'* [an SMS, a policy or process]. Establish is used for the setting up of [something], after it has been defined. Establish is then followed by 'implement' – *'to carry out, fulfil or perform'*. It is always used for 'implement an [SMS, a plan or process]'. To differentiate, a service or release is 'deployed', where the meaning is the normal English language meaning of *'to organize and bring into use'.*

Use of tools

The generic, broad-based approach of the 20000 series means that there are no requirements on the use of tools or other supporting system. A service provider could fulfil all the Part 1 requirements without any tools at all.

In practice service providers use a wide range of tools to assist them to fulfil Part 1 requirements and to deliver the service. This reduces overall costs and risks from errors. Examples include service desk logging and reporting tools, performance monitoring tools and configuration

management databases (CMDBs). If tools are used they become an integral part of the SMS. Although the tools will not be audited their output will be.

Chapter 2 Scope definition

Introduction

This chapter describes scope definition and why it is important.

A scope statement is required for an external audit and for the certificate awarded after a successful audit. However, final preparation for an audit is far too late for the scope of the SMS to be defined. The scope should have been defined earlier as it is used for the planning of the SMS, as described in Chapter 3. The definition of scope establishes a shared understanding of the processes within the SMS and the services delivered to customers.

The scope of the SMS is complex when parts of the service originate from groups outside the service provider's direct control. Typically, this is when part of a service is provided by a supplier under a contractual arrangement. When this is the case the processes should be under the governance of the service provider.

Which groups are in or out of scope?

Many groups and organizations can affect the scope of an SMS. Organizations or groups outside the scope of the SMS usually provide input to the SMS or receive output from the SMS. Many do both.

Key point

A group is outside the scope of the SMS if they are not under the direct control of the service provider. The service they contribute may be in the scope of the SMS and in the audit, but the 'out of scope group' will not be audited. The contribution of the 'out of scope group' is assessed using information held by the service provider. Providing the information should be an obligation placed on the group, e.g. under a contract between the service provider and supplier.

Part 1 includes references to the types of organization, group or person described below. Each is in or out of scope according to the degree and nature of control that the service provider has over their actions.

1. ***Customer*** is an organization or part of an organization that receives services. A customer may be external to the service provider's organization or part of the same organization. Customers are most easily equated to a manager or group of managers with responsibility for agreeing the service from the service provider. There may be multiple customers and multiple services or shared services. Customers may pay for the service or it could be treated as an overhead. Customers are outside the scope of the SMS, and will not be audited even if the name of their organization or services is used in the definition of scope.
2. ***Customers acting as suppliers*** are groups that rely on the service but who also contribute to the service. For example, a special business support group where the service provider depends on an input from the customer. A customer is managed by service level management (SLM) when acting as a supplier. Customers acting as suppliers are outside the scope of the SMS and are not audited.
3. ***External organization*** is an organization that needs to access, use or manage the service provider's information or services. This term is used only in Part 1, Clause 6.6 because of the close link to the ISO/IEC 27000 series.
4. ***Interested parties*** are individuals or groups having a specific interest in the performance or success of the service provider's activities, e.g. customers, owners, management, people in the service provider's organization, suppliers, bankers, unions or partners. They are in or out of scope of the SMS according to the reason for their interest.
5. ***Internal groups*** are part of the service provider's own organization. They can contribute to any stage from planning and design, through to withdrawal of services. They are not under the direct control of the service provider and their contribution is managed by SLM. They are not in the scope of the SMS and are not audited.
6. ***Lead suppliers*** are suppliers responsible for managing other suppliers, referred to as sub-contracted suppliers. Like suppliers, lead suppliers are managed by supplier management. Like other suppliers, lead suppliers are outside the scope of the SMS and are not audited.
7. ***Other parties*** is a collective name for any one or all of an internal group, a customer or supplier, including lead suppliers and customers acting as suppliers. All are outside the scope of the SMS and are not audited.
8. ***Service provider*** is an organization that manages and delivers services to the customer. The service provider may be part of the same organization as their customer, often an in-house IT department, or part of a legally separate organization, such as a commercial outsourcer. The service provider may be aiming to achieve certification to Part 1.

9. ***Sub-contracted suppliers*** deliver services via a lead supplier, and are managed by the lead supplier, not the service provider. The service provider may ask a lead supplier for evidence of competent management of the sub-contracted suppliers. They are outside the scope of the SMS and are not audited.
10. ***Suppliers*** are an organization or part of an organization that is external to the service provider's organization. Each is a separate legal entity and has a contract with the service provider to contribute to the service. This may be design, transition, delivery and improvement of services or processes. Suppliers may operate processes on behalf of the service provider, but cannot have governance of those processes. Suppliers are managed by supplier management and are outside the scope of the SMS and are not audited.
11. ***Users*** are people that relyon theservices on a day-to-day basis, but are not normally directly involved with the service provider. They are outside the scope of the SMS although the name of their organization may be used as a parameter for scope definition, as described below.

Scope definition parameters

Scope may be defined in a number of ways. The rules are the same if the service providers and customers are part of the same organization (in-house services) or are separate legal entities (usually under a commercial service arrangement).

The service provider should use parameters to define the scope of the SMS so that it is clear what is included and excluded. It is common for several parameters to be used in combination. To aid clarity, it can be useful to state what is outside the scope. The service provider does not need to own the assets used for delivering the services in scope. If the scope changes, so should the parameters, e.g. a new customer or service, or the removal of either.

Part 1 does not limit the parameters that can be used. Two are required in all scope definitions:

- organizational units providing services, e.g. a single department, group of departments or all departments;
- services offered, e.g. a single service, group of services or all services, financial services, retail services, email services.

Other useful examples that should be considered include:

- geographical location from which the service provider delivers the services, e.g. a single office or group of offices, regional, national or global;

- customers and their locations, e.g. one customer, many customers, external customers or internal customers;
- technology used to provide the services.

Many more examples are included in Part 3.

Key point

When defining the scope it should:

- be as simple as possible;
- be understandable without detailed knowledge of the organization;
- contain enough information for use in conformity assessment;
- define what has been included within the scope;
- not imply that something is included if it is excluded;
- exclude activities where there is no evidence for conformity to Part 1.

Scope statement for an audit

The scope definition becomes a scope statement for an audit certificate. It therefore should not include the names of other parties contributing to the delivery of the service.

During a certification audit, if the scope definition includes many customers, services or locations, then an assessor will base the assessment on a sample, using his/her professional judgement for selection of the sample and what will be assessed. The scope statement may include the full range of customers, services and locations within the scope of the SMS, not just those sampled during the audit.

Conversely, a service provider can opt for a scope that does not include all their customers. This is acceptable as long as all the requirements are met and the scope statement issued by the auditor makes the limits to the scope clear.

A certification scheme can include rules on the way a scope statement is worded, e.g. a restriction on the type of parameters that can be used by the service provider or that the scope statement should include a reference to the SMS. This is a certification scheme issue, but it is still

based on Part 1 requirements. It is unlikely that a scheme owner will limit the take-up of their scheme in this way, unless it is a sector-specific scheme.

A scope statement on an audit certificate should not include parameters that extend the scope of the SMS beyond the 20000 series. For example, consultancy services on the 20000 series cannot be certified, however competent the consultants. Nor may professional services such as software or systems development. This is the case however closely they work with the service provider and even if they are legally part of the same organization.

Key point

A service provider can implement a process, such as incident management, for all services. If they have only implemented capacity management for one service, the scope statement is limited to that one service, because all requirements should be fulfilled. The incident management applied to other services will not be audited. Only the occurrence in scope will be audited. This circumstance often occurs when a service provider opts to develop the full SMS incrementally, as described in Chapter 4.

The suitability of the scope statement will be decided on its own merits by the audit company that performs the audit. This is done formally during the audit. However, the scope statement is also discussed during the audit sales and planning stage. It is normally included in the contract between the service provider and the audit company.

Key point

The audit company may use other parts of the 20000 series during training or for development of their scheme rules, e.g. Part 3. Despite this, only the requirements of Part 1 are used as the basis of audit decisions. This includes decisions on the suitability of the scope of the SMS.

An auditor will also take into account the rules of the particular certification scheme being used for the audit. The auditor will not take into account anything outside the defined scope of the SMS, such as service and locations out of scope, or processes not under the governance of the service provider.

Evidence should be available to support the validity of the defined scope.

- All groups, departments or organizations involved, what each is responsible for and who has authority and accountability.
- The interfaces between organizations, including suppliers and customers should be defined and agreed.
- Successful integration of processes, including the Plan-Do-Check-Act (PDCA) cycle (also known as Deming or Shewhart Cycle).
- Governance of the processes within the scope of the SMS, whether operated by the service provider or other parties.

Supply arrangements

Any service provider that can provide evidence of meeting all requirements in Part 1 directly can achieve certification. In this case all evidence is based on their own activities. This is rare and applies only if the service provider does not rely on other parties for any part of the service.

Many examples of multiple supplier arrangements exist, often referred to as 'smart sourcing', 'selective sourcing', or 'right sourcing'. In reality, achieving certification is usually dependent on evidence of effective control of other parties, including suppliers, internal groups and customers acting as suppliers.

The contribution made by other parties can be planning, designing, developing or delivering a new service. It can be from a specialist support group or from providing hardware or software. It is increasingly common for this to include Internet-based services used by the service provider's customers and users.

Key point

Customers acting as suppliers can be part of the customer's organization for many reasons. This can be when the customer has bought a core service from a commercial service provider but retained direct control over business-critical skills.

The service provider may find managing the relationship with the customers acting as suppliers requires considerable diplomacy. For example, the service provider is still required to demonstrate they have governance of the processes operated by the customers acting as suppliers.

This includes control of what and when process improvements are made.

The complexity of the supply arrangements is often understood only when the service provider defines the scope of the SMS for the first time. The most common form of complexity is due to the suppliers–service provider–customers supply chain, described in Chapter 9.

This applies even if the different legal entities work very closely together and function as one large organization. The requirement to be a single legal entity also applies to other management system standards, such as ISO 9001.

Key point

A service provider might have to limit the scope of the SMS for certification, e.g. only one location, one service or one customer.

In some cases it isnot possible for all organizations to develop even a limited scope for certification. This can be because the service provider has long-term contracts with suppliers that prevent the service provider having control over all processes in Part 1, Clauses 5 to 9, as required by Clause 4.2. This can also be because the SMS is incomplete, e.g. a process has not been implemented.

Whatever the reason, an SMS is still the most effective way of managing services.

Part 1 does not require other organizations in the supply chain to comply with Part 1 in order for the service provider to achieve certification. An audit is based only on the service provider's own evidence. Other organizations in the supply chain are not audited.

Governance of processes

The requirements of Part 1, Clause 4 should be met by the service provider.

There are additional requirements in Part 1, Clause 4.2 for the service provider's governance of processes operated partly or completely by other parties. These are suppliers, internal groups and, in some cases, customers acting as suppliers.

A service provider planning to use other parties to operate any of the processes in Part 1, Clauses 5 to 9 has one of two options.

- The service provider designs the processes in Clauses 5 to 9 before outsourcing the operation of the process, and includes their governance of the processes in the agreement with the other party.

or

- If the processes in Clause 5 to 9 are already operated by other parties, the service provider should ensure the contract allows them to demonstrate governance of these processes. If necessary, the service provider should agree changes to the contract or documented agreement.

Unless the service provider implements one of these options they will not be able to subsequently fulfil the requirements for governance of processes operated by other parties.

Although Part 1, Clause 4.2 is relatively short, it is exacting. If the majority of processes in Clauses 5 to 9 are operated by other parties, the service provider is unlikely to be able to demonstrate the required standard of governance. However, if other parties operate only a minority of processes, or parts of processes, the service provider is more likely to be able to do so.

Key point

The service provider and suppliers or customers cannot all demonstrate governance of the same processes, using the same evidence.

It may be possible to provide evidence based on another occurrence of the same process, e.g. where the same process is used for two different customers.

The type of evidence required for Part 1, Clause 4.2 should demonstrate:

- process accountability and authority to require adherence;
- process and interface definition;
- process performance/compliance with requirements;
- controlling process improvements.

Top management remain accountable for all processes that are operated by other parties. This is irrespective of the terms of a contract between a supplier and service provider. Nor can this requirement for accountability be avoided due to the terms of the documented agreement between internal groups and customers acting as suppliers and the service provider.

The service provider should be able to show evidence of the active involvement of their managers responsible for each process, irrespective of which organization operates each process.

Evidence includes the identities of managers with authority and responsibility for processes and services.

The service provider is responsible for the effectiveness of all the processes, including process design, interface definition and process improvements. To do this it should also be clear which person is responsible for each process. This is independent of the person who operates the process.

The service provider should ensure each process delivers the expected outcomes and contributes to the SMS, meeting the service management objectives.

The service provider also enforces the process being followed for each service within the scope of the SMS.

Example – Separate legal entities

For financial reasons an organization is split across several companies and is owned and managed by a single umbrella company. Can the separate companies share an ISO/IEC 20000 certificate?

Separate companies cannot share a certificate. This is the case even if the companies are all owned by the same single umbrella company. Certificates can only be awarded to a single legal entity. However, the umbrella company may be eligible for a certificate with a suitably detailed scoping statement. This is also the case with other management system standards, such as ISO 9001 and ISO/IEC 27001.

Does that mean the whole organization has to be audited, including all the separate companies managed by the umbrella company?

No, as long as the SMS scope fulfils all Part 1 requirements only the service provider is audited. This is quite common with very large organizations.

What does each company have to do if they each wish to have their own ISO/IEC 20000 certificate?

Each company would be audited separately and each would have to meet the requirements. This might mean one or more are unable to meet the Part 1 scoping requirements or might not pass the audit. Each company that does pass an audit will have a separate certificate defining the scope of their audit.

Chapter 3 What is an SMS?

Introduction

This chapter describes the key features of a successful SMS. An important and early step is to agree the scope of the SMS, as described in Chapter 2.

An SMS is used to direct and control the service management activities of the service provider. It includes policies, objectives, plans, processes and documentation such as procedures. It defines the resources required to operate the SMS and deliver the services, such as technology and personnel. Each component of the SMS is an interrelated or interacting element, which adds the most value when they all operate collectively. The SMS as a whole defines everything required for the design, transition, delivery and improvement of services.

The requirements for an SMS are in Part 1, Clauses 4 to 9. Clause 4 is the longest clause and covers the initial establishment of an SMS, the continual improvement cycle, management responsibilities, documentation and governance of processes operated by other parties. The remainder of the SMS is the service management processes specified in Part 1, Clauses 5 to 9.

The service provider's strategy

The most effective service providers consider the impact on the SMS through all stages: strategy, design, transition, operation and continual improvement. Although Part 1 has no requirements for a service provider's strategy it has requirements for a service management plan. Many service providers will use their service management planning to set their strategy for the SMS and services. This will in turn generate strategic and tactical plans to be executed at all stages.

Part 1 uses the term 'service requirements' for the needs of the customer(s), users and the service provider. The service requirements also shape the service provider's strategy.

Management commitment

An SMS will only be effective if it is supported by top management. Some top managers do not immediately realize how many benefits there are from adopting best practices: efficiency, effectiveness, increased customer satisfaction, better service levels, faster changes, lower unit costs.

Commitment can often be gained by presenting the benefits of implementing an SMS based on Part 1, rather than emphasizing only the risk of failing to meet statutory and regulatory requirements or contractual obligations.

Top management is normally aware of statutory and regulatory requirements and contractual obligations and that their continuing employment can depend on fulfilling these. This can influence their willingness to demonstrate commitment themselves and encourage those people they manage to also have commitment.

Top management should also understand that they are directly responsible for the whole SMS and also accountable for processes operated by other parties, under Part 1, Clause 4.2.

Key point

> The most effective top management understand the importance of their commitment to the SMS. They become directly involved in establishing the scope, policy and objectives for service management. They also have a central role in communicating the importance of the SMS and delivering services to satisfy customers. Top management also ensure that an SMS does not degrade once the novelty of the initial project establishing the SMS has faded away.

There is an inextricable link between top management commitment and provision of the resources required for the SMS. This is not just in the early stages of planning and implementation but also that the resources required are retained over time. Top management should not move resources to another project or service without understanding the impact on the SMS.

Sustaining an effective SMS requires a top management communications programme. Good intentions are not enough – the communications should be defined in procedures and actually followed, as described in Chapter 6.

What do managers want?

Part of top management's responsibilities are objectives and policies. These are used to identify what is required of the rest of the service provider's organization. Correctly written, they give goals for planning the SMS and continue to provide direction whilst the SMS is operated and services are delivered.

The service management plan, described in Chapter 4, defines the way the objectives and policies are used. The plan prevents changes to the SMS having an adverse effect. The plan ensures the improvements are optimized and given a suitable priority.

Objectives and policies are effective for cascading top management direction through the organization. This direction should include commitment to meeting service requirements and continual improvement of the SMS and services.

Policies only make a difference if they are under pinned by process and procedures (i.e. what people actually do), as shown in Figure 1.

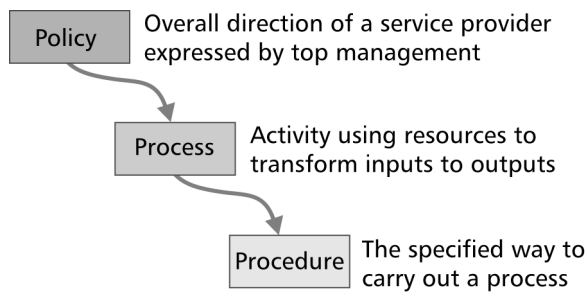


Figure 1 – Policy, process, procedure

If the objectives, policy, process and procedures are out of alignment they are realigned using the improvements from 'Plan-Do-Check-Act', described below.

Risk management

Risks arise from many causes. Major changes, unexpected disasters or attempted fraud are all examples. It is possible that the service provider's personnel, customers or users can accidentally or intentionally introduce risks. This can be because they have not understood the impact of what they do on the rest of the SMS or on the services delivered to customers.

There is no separate risk management process in the 20000 series. Despite this, understanding and avoiding risks is fundamental to the 20000 series. In the worst case the service provider should accept the risk and also manage the impact of any risk that has resulted in a failure. Top management is closely involved in this.

Management reviews and internal audits

The need to understand, avoid or manage risks is why activities such as reviews or internal audits feature in several Part 1 requirements. For example, Part 1, Clause 4.5.4 requires top management to be involved in formal management reviews and to support internal audits of the SMS. Although Part 1 refers to '*planned intervals*', simply scheduling reviews as a routine matter is inadequate. Both the management reviews and internal audits should be considered constructively and carefully and done at sensible intervals. 'Sensible' varies according to the service provider's circumstances and can change over time.

Key point

Planning a review to take place at long but planned intervals could seem to superficially fulfil Part 1 requirements, but then fail under an auditor's *'is this sensible?'* test. The frequency should prevent the SMS and service degrading significantly between reviews. Conversely, arranging frequent reviews 'just in case' indicates too little thought about what is needed. Overly frequent reviews, especially during a period of stability, will introduce an overhead but deliver little benefit. The correct frequency will depend on the service provider's circumstances. Few service providers will find once a year is adequate and for those managing many changes a greater frequency is required.

During management reviews and internal audits, policies and objectives are checked to ensure they are being met and remain fit for purpose. This is particularly important if there are major changes to services or to the service provider's organization. The knowledge and experience of top management plays an important part in this.

Delegation of authority and responsibility

Top management may delegate some authority and responsibility to other managers, starting with the design of integrated processes to meet the policies and objectives. Delegation can also include ensuring statutory and regulatory requirements and contractual obligations are met.

Process owner

Although Part 1 does not use this term, an important example of delegation of authority and responsibility is often referred to as the role of 'process owner'. This is a manager responsible for the quality of a process and can be vital to ensuring the SMS is operated to a high standard. Being allocated this role generates a strong sense of personal involvement and increases middle and junior management commitment. The benefit is close attention to process and service quality. This type of role is also fundamental to process governance, under the requirements in Part 1 Clause 4.2, described in Chapter 2.

An effective process owner takes a wide view of their process and the way it relates to the rest of the SMS. They also ensure that the output from one process is available when required by another process.

Many service providers, and in particular small organizations, ask one person to have responsibility for more than one process. This is effective as long as overall priorities are understood and the manager selected has the correct skills and temperament to be effective for all 'their' processes.

Key point

Ultimately, top management have an incentive to make sure delegation is effective. They should require reports on progress and the identification of opportunities for improvement to the SMS and services. Top management then drive through agreed improvements. They check that their delegation of responsibilities is effective. Where the delegation of responsibilities has not had the desired results top management can establish why not and what should be done. Top management should remain aware of the difference between abdicating and delegating responsibility.

Organizational structure

Part 1 does not include requirements for a specific organizational structure and the way process ownership and improvements relate to operational responsibility. Service providers with widely differing organizational structures are certified to 20000.

The simplest structure is a complete process contained within a single unit of an organization, even if there are interfaces between that process and others. In reality a process is normally operated across several organizational units. For example, as shown in Figure 2, incident management crosses the organizational boundaries to two suppliers as well as boundaries within the organization.

It is important to be clear on the processes, procedures, roles and responsibilities for each process and each person because they usually cross organizational boundaries

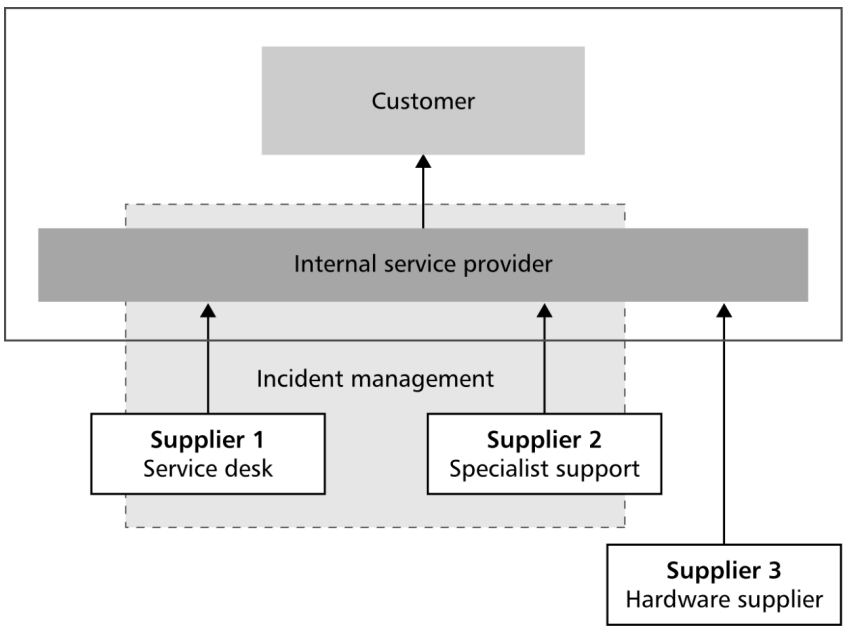


Figure 2 – Processes spanning organizational boundaries (based on Part 3)

All too often one organizational unit changes the way it operates without understanding how this affects other units, e.g. changing a supplier's contract without realizing it prevents the service provider's

governance of processes operated by the supplier. Changing organizations due to the SMS can affect the personnel involved, as described in Chapter 6.

Key point

The roles of process owner and an operational manager are different, even if the same person is allocated both roles. For example, a service desk manager can be the process owner of incident management and have responsibility for improvements to the whole process. The service desk manager's operational role is limited to the service desk with no operational responsibility for incident management elsewhere. In this case the service desk manager is responsible for process improvements outside their operational unit.

Plan-Do-Check-Act

The PDCA cycle is used to initially set up an SMS and then to continually improve the SMS and services. This is comparable to other management system standards, such as ISO 9001. The PDCA cycle is illustrated in Figure 3, below.

Plan

The plan is based on the agreed scope of the SMS, as described in Chapter 2. The plan establishes the way the objectives are to be achieved and influences the design of the processes. After the implementation of the SMS the planning stage then identifies improvements to the SMS to address gaps, issues and to mitigate risks identified in a previous check stage.

Do

This stage is the establishment, implementation and operational running of the SMS and services. This ranges from allocation and management of agreed funds and budgets through to monitoring and reporting on the performance of day-to-day service management activities.

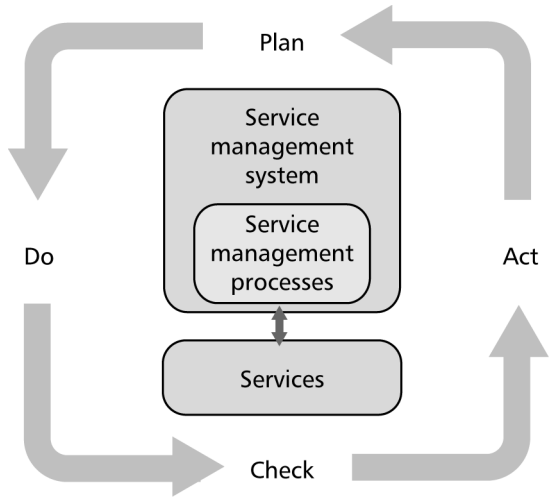


Figure 3 – PDCA and service management from Part 1

Check

There are two important aspects to this stage: internal audit and management review of the SMS. Internal audits are planned and performed by people independent of the SMS being audited. The SMS is checked to see if it has been correctly implemented against the requirements in Part 1 and against the service requirements. The internal audit also checks that improvements to the SMS or services have been successfully implemented.

Management reviews are similar, but are from the viewpoint of the service provider's managers and the customers. The reviews also take into consideration changes that have or could affect the SMS and services. This stage checks on actions identified in previous Act stages. It includes communication of the results of internal audits and management reviews to interested parties.

Act

This stage is both the maintenance of the SMS and its continual improvement. Clarity on 'who does what and when' is essential for both maintenance and improvements, including any corrective action. The benefits of improvements and other changes to the SMS are monitored against plans and targets.

Continual improvement

The continual improvement cycle based on PDCA is fundamental to the 20000 series. The integration of the SMS means each process contributes to the continual improvement cycle. For example, processes, such as incident management, contribute mainly by providing data whereas the proactive processes, such as change management, can contribute directly to identify improvements. One of the biggest challenges for any service provider is establishing a culture of continual improvements for sustainable success. Continual improvement is referred to throughout this book.

Integration of processes

A process operated in isolation is only slightly better than no process at all. An SMS is only truly effective if processes are integrated by information flowing between them. Some process integration, e.g. of change and configuration management, are a Part 1 requirement, because they are fundamental to the SMS as a whole. However, on the whole, what information flows between processes is largely dependent on the service provider's circumstances, the policies that the processes underpin, and on the actual detail of procedures that in turn underpin the processes. Integration of processes is described in Chapters 4 and 5.

Chapter 4 Establishing an SMS

Introduction

This chapter describes planning for the design and establishment of an SMS that will conform to Part 1 requirements. Part 1 does not specify any particular project management method, but establishing an SMS should be managed as a project or a programme of projects.

The key features of establishing an SMS are summarized at the end of this chapter.

The service management plan

Part 1 uses the term 'service management plan' to mean much more than a Gantt chart. The service management plan is a set of documents used during the initial establishment of the SMS, then during operational running and continual improvement of the SMS and services. The plan is developed and changed over time, not just used for the initial establishment of the SMS.

The service requirements drive the service provider's strategy and shape the service management plan.

The contents of the plan can be held in one physical place or held physically separate but logically linked. It is common for service requirements, resource plans, budgets and accounting documents to be physically separate from but logically linked to the plan.

The features provided by intranet-based systems makes the logical linking an easy and useful approach. However the information is structured and held, the contents are typically those listed in the checklist below.

Checklist for the service management plan

- Service management objectives to be achieved by the service provider
- Policies
- Authorities and responsibilities for the service management plan
- Statutory and regulatory requirements
- Contractual obligations to customers

- Contractual obligations of suppliers and lead suppliers
- Commitments of internal groups and customers acting as suppliers
- Standards, including ISO/IEC 20000-1
- Service requirements, linked to the service catalogue and service level agreements (SLAs)
- Known limitations that can impact the SMS
- Roles and responsibilities for processes and procedures
- Accountability for processes operated by other parties
- Identity of other parties operating service management processes
- Identity of external organizations with access to information or services
- Approach to be taken for working with other parties, including suppliers, internal groups and customers acting as suppliers
- Approach for the management of risks and the criteria for accepting risks
- Technology used to support the SMS
- Resources required: human, technical, information and financial
- How the effectiveness of the SMS and the services will be measured, audited, reported and improved

Gap analysis

The service provider should perform a detailed analysis to evaluate the gap between the current operations and the requirements of Part 1, for the activities in the defined scope of the SMS.

The results of the gap analysis should be used to decide if existing service management is a suitable basis or if a new start is more likely to succeed.

A gap analysis checklist is given below, based on Part 5.

Gap analysis checklist

a) Scope and details of any management system(s) already established
b) Existence and quality of documents and records, including:
    1. policies, processes, procedures and objectives;
    2. service catalogue and service level agreements;
    3. supplier contracts;
    4. formal agreements with other parties;
    5. evidence of governance of processes operated by other parties;
    6. records of achievements by the service provider;
    7. records of achievements by other parties, including suppliers.
c) Actual working practices
d) Management reviews

e) Internal audits
f) Conformity assessments (e.g. ISO 9001, ISO/IEC 27001)
g) Service reviews
h) Actual service levels
i) Recent or current service improvement plans
j) Documented and actual roles, responsibilities and authorities
k) Skill and competence requirements versus actual achieved
l) Headcount actual and budgeted for in the current and next year
m) Organizational structure of the service provider
n) Description of customers' business activities
o) Details of recent serious complaints and satisfaction surveys
p) Assessment of the service provider's culture
q) Any major changes planned to the structure, service and/or technology
r) Statutory and regulatory requirements
s) Contractual obligations

Where to start?

A decision should be taken whether the established practices are to be left unchanged, amended or completely replaced.

It can be difficult to correct existing practices when service management processes have been implemented in isolation, are incomplete, documented badly or are not operated consistently. Existing processes can also need changing so that they are integrated.

History plays a part, e.g. if earlier initiatives have been failures. A new SMS allows the service provider to leave the history of past failures behind.

Top down or bottom up?

Many service providers find it is more effective to design and establish an SMS as a new initiative, starting with a clear view of what is to be achieved by implementing the SMS.

The first step for this top-down approach is defining the scope of the SMS.

The next step is agreement of service management policies and objectives, providing the overarching principles for the integrated service management processes.

The plan stage of the PDCA cycle covers both the initial planning of the SMS and then provides the basis for continual improvement from later PDCA cycles.

The 'bottom-up' approach to establishing an SMS is based on incremental growth of processes already in place. This mainly occurs when top management have not yet understood the value provided by a fully implemented or integrated SMS. In these cases the establishment of the SMS is left to junior personnel who are enthusiastic but do not have the power to bring about the scale of changes required.

The role of top management is so important to success of the SMS that it is necessary to correct this misunderstanding promptly.

Example – who can be certified?

An organization does not have all of its processes in place, although the ones that do exist have been implemented to a high standard. Can they become part-certified?

No, they may not.

Although it is not compulsory for the whole of an organization to be included in the scope of an SMS and the audit, all processes in Part 1 should be in the scope and all requirements contained in Part 1 should be fulfilled.

All Part 1 requirements are compulsory. Part-certification for just some of the processes is not possible.

Phases for implementing a single SMS

It is advisable to implement an SMS using phases of linked improvements, such as shown in Figure 4. Only part of the SMS is implemented at each phase. Each phase should bring benefits that encourage involvement for the next phase, including funding the next phase.

Part 5 provides advice on phases for implementing an SMS. Service providers should adapt the plan to suit their circumstances, based on the gap analysis described above. The three phases are suitable whatever the scope of the SMS.

Table 3 shows the main objectives of each phase. The service provider cannot fulfil all Part 1 requirements until the end of Phase 3 and is therefore only able to be certified at the end of Phase 3.

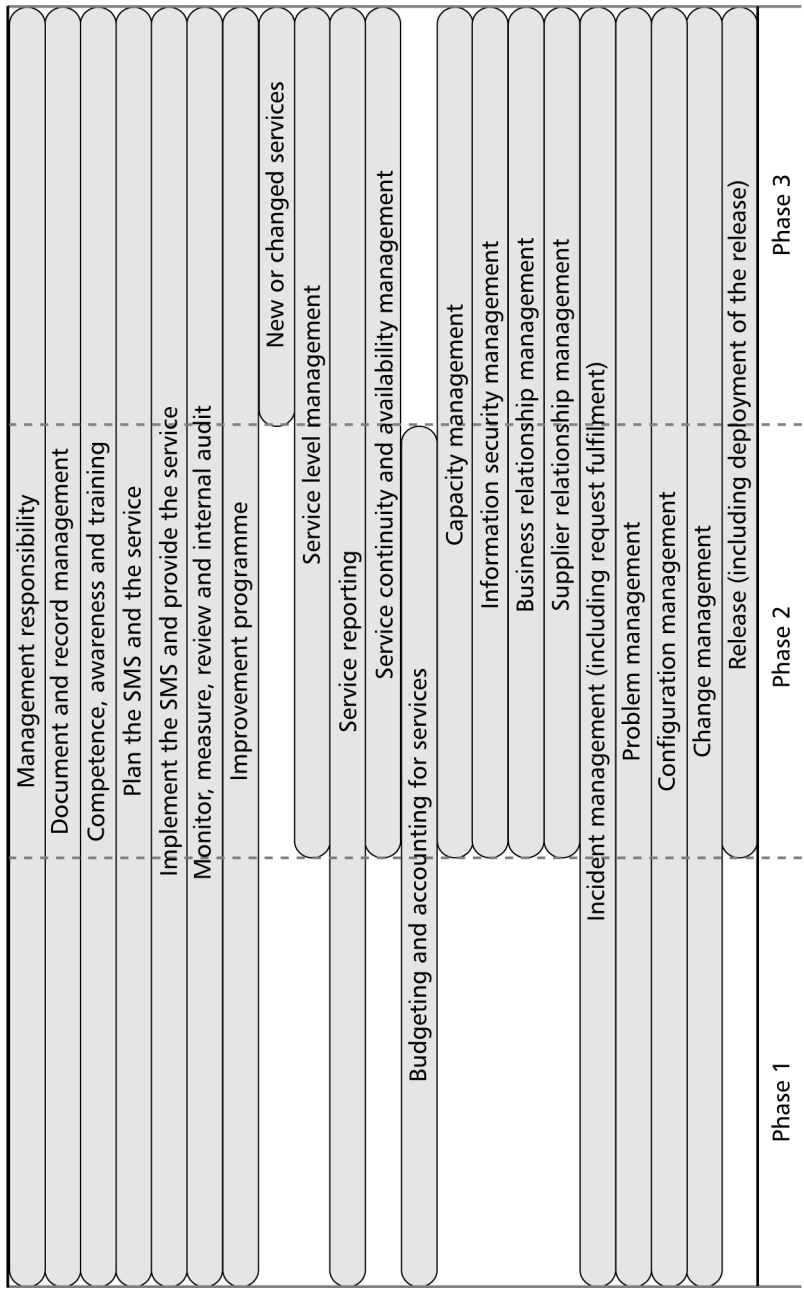


Figure 4 – Part 5's three phase approach for an SMS

Table 3 – Objectives of each phase, based on Part 5

Phase 1	Phase 2	Phase 3
Incorporates the findings of the gap analysis and the business case.	Adjustment of plans based on achievement analysis at the end of Phase 1.	Adjustment of plans based on achievement analysis at the end of Phase 2.
SMS structure implemented including the plan, initial policies, commitment/ accountability, crisis management/ reactive processes.	Revision of policies, additional processes, integration of existing processes, procedures and other supporting documentation.	Revision of policies, final processes (proactive), integration of all processes, documentation of underpinning procedures and supporting documents.
The service provider will have implemented policies, processes and procedures to fulfil the requirements of Part 1 for a basic SMS, with the focus on reacting quickly and effectively to service disruptions and requests. The service provider has knowledge of all the services that enable it to react to service disruptions or requests.	The service provider will be able to anticipate and avoid service disruptions and requests on completion of Phase 2. The service provider will have stabilized its processes and activities in order to provide a more reliable service to its customers. It will have begun discussing with its customers their future service requirements, in order to incorporate their needs into its plans.	There will be a service culture and a good understanding of the customer's business and service requirements. Measurement of the effectiveness and efficiency of the services and processes will be used. Continual improvement of delivered services will be established. Relationships with suppliers and customers will be established.
By the end of Phase 1 the SMS will provide the basis for Phase 2.	By the end of Phase 2 the SMS will provide the basis for Phase 3.	By the end of Phase 3 the SMS will provide the basis for stabilization and continual improvements.

An incremental approach to the SMS

The scope agreed early in the project might have to be revised at a later stage of planning. For example, a service provider can decide to define the scope as 'all services, locations and customers'. Then, when the risks and short-term costs are better understood, switch to an incremental approach, starting with a small number of services or a single location.

This reduces risks by first establishing an SMS of limited scope, then later extending the scope after experience is gained and best practice processes become the norm. A single large project to fulfil all requirements can be higher risk and be difficult to fund if there is scepticism about the scale of benefits.

Key point

> An incremental approach is the staged increase in scope of the SMS. It is not phased fulfilment of Part 1 requirements. For each incremental stage of establishing an SMS all requirements should be met at each stage.

An incremental approach to extending the SMS allows costs to be incurred over more than a single accounting year, which is generally easier for funding. It can also be possible to fund some costs out of operating budgets, i.e. revenue budgets, instead of completely funded by capital. The difference between different budgets and cost types is described in Chapter 11.

The rare exceptions will normally be where there is an urgent regulatory or commercial need to 'achieve 20000 quickly'. Even then there should still be a sensible sequence of activities and Part 5 will provide useful advice.

The project team

The team should be balanced between personnel with experience of the status quo and those that are willing to adopt new practices. The project should not be completely reliant on people who also have operational roles because this can cause resourcing conflicts, especially for a large project.

The project team should have expertise in:

- designing and implementing management systems;
- process definition;
- process establishment, implementation and integration;
- minimizing impact on day-to-day activities;
- testing and measuring the effectiveness and improvements of processes;
- organizational change and communication.

Top management, managers with responsibilities for process quality and operational line managers all play an important part in identifying and encouraging adoption of new practices and attitudes.

Key point

The service provider does not have to use the process names in the 20000 series. Using existing names or avoiding process names that have previously been associated with difficulties can minimize the scale of changes for the organization. This can help deliver benefits earlier and more easily. Mapping the Part 1 names to the actual names will help during an audit.

Operational managers are often risk averse, so can be reluctant to adopt changes, experience having shown them that change is a risk and problems arise when there is a risk. However, they are important as they bring to the project a strong measure of practicality.

Policies

The relationship between policy, process and procedure, described in Chapter 3, is one of the most important aspects of designing and implementing best practice service management. The project manager should keep this in mind at all stages, or risk implementing a fragmentary and inefficient SMS.

Key point

Policies may vary in detail and scope according to the service to be provided. Policies that meet the needs of one organization will not necessarily meet the needs of another. The document could have a title other than 'policy', but if it provides suitable management direction it serves the purpose of a policy. It can be presented as evidence of policies, during an audit.

The importance of policies does not imply the need for a long, complex document. Long policy documents are often the result of policy, process and procedures being merged and incorrectly referred to as a 'policy'.

Many organizations have an incomplete set of policies. The policies in existence often cover issues such as security, health and safety and use of email, but not the rest of service management. Many policies are not supported by processes or procedures and fail because they have no influence on what people do.

For a service provider developing policies for the first time, or improving existing policies, useful input is available in the Part 1 requirements and advice in Part 5.

Example service management policy statements based on Part 5 are given below. The examples are suitable for Phase 3, when the SMS is already established and effective. Policy statements can also be developed during Phase 1 to set direction for Phases 2 and 3.

Service management policy statements

- Service management aims to deliver services to agreed service requirements and create value for customers.
- The SMS is maintained under the Part 1 processes and procedures.
- A co-ordinated set of strategies, policies and plans will be communicated and used to direct service management activities.
- The results of management reviews and internal audits are used for corrective action and improvement.
- The interfaces between management processes are clearly defined, documented and monitored for effectiveness and efficiency.
- Desired outcomes and metrics are defined and metrics are used to measure the effectiveness and efficiency of processes in the SMS.

- Roles and responsibilities are defined in the service management processes in a consistent and complete manner, across all processes.
- Changes to processes or procedures are only made via change management.
- Personnel are trained to an agreed level of competence in the processes and procedures they perform or for which they are accountable.

Service requirements and process definition

The degree of automation should be taken into account. If many activities are manual, processes should be simpler than if extensive automation is possible. It may also be possible to improve the efficiency of the SMS through automation.

The service provider should ensure processes, process interfaces to other components of the SMS and the contribution of processes to service requirements are all documented and achieved. This forms part of the audit evidence for certification, e.g. evidence of the inputs and outputs identified for each process. Integration of processes is described in Chapter 5, documents and audit evidence are described in Chapter 7, design and transition of services are described in Chapter 18.

The central role of the service provider is important if the activities of a single process are operated by several parties. For example, the resolution processes can be operated by several suppliers, internal groups and customers acting as suppliers. All parties are required to adopt processes controlled by the service provider.

Performance reviews

Process performance review involves both management reviews and internal audits. The Plan-Do-Check-Act cycle used for improvements should be applied to all processes at regular intervals. The service provider should use criteria such as the requirements for the process and any process interfaces/integration. The service provider can also do ad hoc checks on processes, e.g. after a major incident or when targets are frequently breached.

If a process is operated by another party the service provider should ensure the other party applies the same cycle of best practices and that improvements reflect the service provider's priorities. This is the case if the other parties contribute to a service in the scope of the SMS, even if the other party is excluded from the scope. It can be necessary to include agreement to this activity into contracts or formal agreements between the service provider and other parties.

The service provider can be asked during a certification audit to provide evidence of having done checks on other parties. The auditor will check the evidence but not question the other parties directly during a certification audit.

Controlling improvements

Changes can be motivated by the need to improve efficiency, the standardization of processes across different suppliers, or due to a major change to the service. The latter is under Clause 5 of Part 1, 'Design and transition of new or changed services'.

Key point

The service provider's evidence of governance of processes includes showing the application of the PDCA cycle to any process, including those operated by other parties. This includes the selection of improvements to processes and allocation of priority to the improvements selected. It also includes all changes that affect process interfaces/integration.

Decisions on process design or improvements cannot be left to junior personnel. Parochial decisions made on the basis of what is best for one process can have a disastrous effect on another process. Decisions on changes to processes should always involve someone who has sufficient authority and a broad-based understanding of the whole SMS and an awareness of best of breed processes.

Once a process has been implemented, it can be subject to improvements and other changes. This can affect the process activities, workflow, inputs/outputs and interfaces to other processes. The service provider continues to have accountability for this, but may work with other parties to document and approve changes to processes that another party operates.

Setting up the project – key points

Establish understanding of:

1. Principles, requirements and applicability of Part 1
2. Scope of an SMS, including other parties' operating processes
3. Desired business outcomes including service requirements
4. Objectives of service management
5. Policies for service management
6. Dependencies on other parties
7. Governance requirements
8. Statutory, regulatory requirements, contractual obligations

Business case and project initiation

1. Objectives for implementing ISO/IEC 20000-1
2. Recommendations on formal independent conformity review
3. Proposed scope of the SMS
4. Predicted service levels (or changes to service levels)
5. Predicted changes to workloads
6. Cost savings as overall costs and unit costs
7. Other direct or indirect benefits
8. Estimated project resources, including the project team
9. Interested parties affected by or involved in the implementation
10. Risk assessments and risk management recommendations
11. Terms of reference
12. Top management and interested parties as project sponsors
13. Project governance agreed
14. Project team leader agreed
15. Project team structure and resourcing agreed.

Project planned in detail, including for each phase towards the SMS

1. Timescales and phasing
2. Attitude of managers to changes required to implement an SMS
3. Assessment of the organizational culture and ability to adapt
4. Numbers, skills, competences of implementation project team
5. Financial constraints on funding for the implementation project
6. Accommodation, facilities and tools available for the project
7. Service owner(s) and process owners identified
8. Delegated authority agreed

Implementation project plan, including resources.

What can go wrong during the project?

- No shared understanding of the objectives of service management
- The scope of the SMS is too wide for the time and resources available
- Customers do not believe the SMS will deliver benefits to them
- The objectives in 'going for 20000' are unclear or undocumented
- Service provider cannot demonstrate governance for all processes
- Service provider does not manage suppliers that contribute to the SMS
- Top management provide only nominal support and are not committed
- Top management is not accountable for the SMS and service
- Managers with responsibility for processes are not identified or involved
- Project phases are too ambitious/unrealistic or do not bring benefits
- Agreed resources are withdrawn for other 'higher priority' projects
- Personnel feel threatened by the changes
- Statutory, regulatory requirements have been ignored when planning
- Contractual obligations are not achievable
- Supplier's contractual obligations are misaligned to the SLAs
- Policies do not align with the service provider's objectives
- Policies do not support the service provider's obligations to the customer
- Policies are not understood by the service provider's personnel
- Processes are not directed by the policies
- Processes operate in isolation or process interfaces are not managed
- Procedures are not directed by processes
- Roles, responsibilities, authorities and accountabilities remain unclear
- Documentation is produced that does not reflect reality
- Documentation is excessive and generates bureaucracy
- Documentation is not managed effectively
- Personnel are not trained in the new processes and procedures
- Risks to the project, SMS and service are not understood or managed
- There is no plan for service and service management improvements
- The plan for establishing the SMS is not being managed or reviewed

Chapter 5 Integrating processes

Introduction

This chapter describes process integration for a range of different operating models, with explanations of why integration is so important.

Understanding the information flows between processes is part of understanding the effectiveness of each process and of the SMS as a whole. Without this the service provider is unable to understand the workings of its own SMS and therefore cannot improve it.

Some of the most important integration is across the interfaces between the PDCA processes and the service management processes, as described in Chapters 8–18. Depending on the individual service provider's circumstances, some service management processes in the scope of Part 1 can need information from every other process at some time. Conversely, some service management processes provide information that can be used by every other process. The flow of information between one process and another may be direct or it may be via other processes, according to the individual circumstances of the service provider.

Processes also need to work with the catalogue of services, service components, service provider and customer assets. Integration is most likely to be inadequate when processes span organizational boundaries, especially across boundaries to other parties.

Is there a best way to integrate?

There are many different ways to achieve effective integration between processes. The 20000 series intentionally allows flexibility of approach to integration for the wide range of circumstances faced by service providers. Each service provider should identify the best way to integrate processes for its particular circumstances. This can be different for another service provider. It may also change over time, but should do so under the control of change management.

The integration of processes has to take into account not only the individual processes and their interfaces, but also the people and technology required for effective service management. Part 1 requires

management to be actively involved in the development of competence, awareness and training in service management.

Whatever decisions are made on integration, the service provider is required to document the interfaces and to ensure the integration is understood and agreed by all those involved. Each process and its interfaces should be defined in a way that makes it clear which process collects what information and when it should be collected. Although many options for interfaces exist, those explicitly required by Part 1 include those given below. Interfaces references in Part 1 are listed in the table below.

Table 4 – Interfaces referenced in Part 1

Clause 4, management responsibilities to ensure that the SMS and processes in Clauses 5 to 9, deliver services that fulfil the service requirements.
Clause 4.2, on governance of processes requires the identification of all processes, or parts of processes that are operated by other parties.
Processes in Clause 4.3 on control of documents and records from all other processes.
Clause 5, design and transition of new and changed services and processes in all other clauses for the design and transition activities. There are specific interfaces with: • Clause 4, PDCA cycle; • Clause 9.2, change management; • Clauses 9.1 and 9.3, configuration management and release and deployment management, optionally via change management.
Clause 6.1, SLM and Clause 9.2 change management.
Clause 6.2, service reporting uses information from other processes such as performance against service level targets, detected nonconformities, workload characteristics. Specific interfaces are: • Clause 6.3, service continuity for plans that were invoked; • Clause 7.1, BRM for complaints and customer satisfaction results; • Clause 8.1, incident management for major incidents; • Clause 9.2, change management for information on the deployment of new or changed services.
Clause 6.3, service continuity and availability management interfaces with other processes in planning and testing the plans.
Clause 6.4, budgeting and accounting for IT services interfaces to all other processes and provides information on the costing of requests for change with Clause 9.2 change management.
Clause 6.5, capacity management to define the capacity and performance requirements for each process as well as monitoring capacity and performance.

Clause 6.6, information security management and Clause 9.2 change management.
Clause 7.1, BRM and: • Clause 6.1, SLM; • Clause 9.2, change management.
Clause 7.2, supplier management that works with other processes to define the contractual requirements and obligations.
Clause 8.1, incident and service request management and: • Clause 6.6, information security; • Clause 8.2, problem management; • Clause 9.1, configuration management; • Clause 9.2, change management; • Clause 9.3, release management.
Clause 8.2, problem management and: • Clause 8.1, incident management; • Clause 9.1, configuration management; • Clause 9.2, change management; • Clause 9.3, release management.
Clause 9.1, configuration management receives updates to the CMDB or provides information in the CMDB to: • Clause 6.3, service continuity and availability management; • Clause 8.1, incident and service request management; • Clause 9.2, change management; • Clause 9.3, release and deployment management.
Clause 9.2, change management, uses information from change management and other processes to assess requests for change. Most service management processes pass information to change management, as is shown against the other clauses.
There are requirements for interfaces between the service provider's SMS and processes operated by other parties, specifically: • Clause 6.4, budgeting and accounting for IT services and the other financial management processes; • Clause 9.1, configuration management and the other party's financial asset management.

Understanding integrated processes

For a fully integrated set of processes, data from one process passes to others in an agreed sequence. This happens at agreed times, e.g. daily, on request, when triggered by a specific event. The definition of interfaces specifies what information is passed from one process to another, why and when it is passed to another process.

Process inputs and outputs include information required for the operation of the process. Outcomes include the results of the process, e.g. incident resolution targets are met and capacity is available as and when required.

Integrated service management results from the use of many best practices, which include:

- agreed policies and service management objectives;
- effective service management planning;
- authority and responsibility for the service management plan;
- processes that reflect business needs;
- clarity on the scope and ownership of each process;
- processes that underpin policies and deliver against objectives;
- understanding of process interfaces;
- information flows between processes, as metrics and service reports;
- policies, processes and procedures that can be measured;
- documents and records that are current and controlled;
- staff with clear roles and responsibilities and the correct skills;
- effective use of service management tools;
- overall control by the SMS.

Integrating processes also avoids each process becoming an isolated activity, so that those involved in each process work together, not as disconnected and potentially competing organizational units.

Process changes

Changing one process can affect data that flows across the interface between processes and therefore affect other processes. This effect is sometimes unintended and can produce serious difficulties in operating processes and delivering the service. This is why understanding integrated processes overall is so important.

In some regrettable real life examples a team or manager involved in a process can actually become competitive about 'their process', believing it is more important than any other. As a consequence they can intentionally or unintentionally sacrifice the benefits of overall service management in order to gain short term and parochial benefit for 'their process'.

Typically, these managers are uncooperative outside their department, being very competitive. They can have good intentions, but be oblivious to the impact their changes to process have on everyone else and all other processes.

Key point

Working together

A decision made in isolation by the supplier management process owner can ripple through and impact the service to the customer. This can mean that the service provider's commitments to the customer cannot be met, the customer's business activities are put at risk, customer satisfaction degrades and the relationship between the customer and service provider is damaged.

The reverse is also a risk. A decision on a target in an SLA made by the SLM process can ripple through and impose requirements on a supplier that are not met by the current contract. For example, unrealistic times for a break-fix service being imposed on a supplier.

This type of adverse effect is avoided with an integrated SMS and clear roles, responsibilities and authorities.

A top-down approach to SMS establishment, described in Chapter 4, reduces the risk that those involved are focused only on 'their process'. They are more likely to realize they should understand other processes, what the other processes need and what they could in turn gain from other processes. This promotes understanding of the damage that can be done through parochial behaviour. This works best because processes are developed on the basis of meeting what the SMS should achieve as defined by service management and policies.

Passing control of an activity

It should also be unambiguous at what point responsibility for and control of an activity passes between processes and across organizational boundaries. Two processes cannot be in control of the same information item or for the same activity at the same time.

For example:

1. problem management takes incident data to identify root cause;
2. once the root cause is understood problem management identifies a fix;
3. control of the proposed fix then passes to change management for full assessment of the proposed fix and scheduling.

This understanding is even more important when the service provider is reliant on other parties to deliver part of their services, e.g. by operating processes in Clauses 5 to 9.

Key point

With a shared service model there is the risk that a supplier makes a change at the request of another organization. The other party might not realize the impact of changing the process without consulting all those affected. When this happens the service provider will not only be unable to demonstrate process integration, they will also be unable to demonstrate process governance.

Storing information

However the information that passes across an interface is collected it should be controlled as a valuable resource. For example, SLM and BRM may both collect data that should be available for use as a single logical dataset. In this example, as long as there is a clearly defined, complete, accurate and shared view of the customer's business needs, there can be multiple views or perspectives depending on the context and scope of a process. Processes using fragmented sources of data quickly become misaligned as each process is operating on a different basis. It also represents an expensive overhead.

PDCA and service management

It is particularly important to plan the interfaces between the processes in Part 1, Clause 4 and the service management processes in Clauses 5 to 9. For example, the Clause 4 continual improvement of the SMS and services and the interfaces to the proactive aspects of the service management processes.

Part 1, Clause 4.5.4.3 requirements are for management reviews of the SMS and services at planned intervals, to identify if they are still suitable and effective. This also requires opportunities for improvement to be identified, such as process performance.

So how does this relate to the requirement for service management processes, such as SLM, information security, the relationship and resolution processes and change management all to identify

opportunities for improvement? Which process controls identification of improvements and which process controls the implementation of improvements? The Part 1 requirements allow many different ways to identify and implement improvements.

The key to this working effectively is for the service provider to understand the way each process operates and the way they relate. It is also necessary to have firm overall control by change management of changes made to the SMS and services. This also requires a service management plan. The plan does not have to be based on one single large project; instead it can be a programme of separate co-ordinated projects.

Projects co-ordinated by the overall programme could include local plans for individual processes, locations or organizational units. Where the service provider relies on local, process-specific plans, these should be compatible with and under the control of the overall service management plan.

There should be no conflicts over the local plans, other process-specific plans or the activities of the PDCA cycle. However process changes are planned, each change should not have a detrimental impact on other processes. This requires information to flow between local, process-specific plans and the PDCA cycle. Many service providers manage their process-specific plans under the umbrella of continual service improvement programme management.

Where there is a holistic view of the service requirements, the SMS and what services are to be delivered, it is easier to have an overall view and control of changes. This is because the most vital information for the SMS is held, and it is possible to assess how one change to a process will impact the rest of the SMS.

One method is to pilot changes where and when possible, so that experience can be gained and fed into the next stage of planning as ‘lessons learned’.

Changes to business needs

Information on business needs and views on the existing service may be obtained from a number of sources. For example, information can be obtained by discussions with the customer and from satisfaction surveys. The service provider may also do market research. This is particularly relevant where the service provider is delivering consumer services. Examples include an Internet or a telecommunications service, with many individual customers.

Although there are many sources of information on business needs, collection of the information should be based on information flowing across well defined and managed interfaces between the processes. Lack of control and consistency in the way the information is collected introduces increased errors and gaps in knowledge. Collecting information works best when it is linked to a specific need, such as the development of policies and processes. For some, such as capacity, service continuity and availability management, an understanding of the customer's business needs is used for the management of risk to the services.

The information on the customer's business needs may be collected by more than one process and used by more than one process.

Where the customer's business needs are not articulated, service providers need to understand the nature and dynamics of the business environment, challenges, and opportunities faced by the customers. This is most common with consumer services with many individual customers.

Changes to business needs can have a wide-reaching effect, e.g. a planned or expected major change to a customer's business activities can require many changes to service requirements.

The change to service requirements ripples through the SMS. It is important to understand the way this information is passed from one process to another.

Key point

Other questions that need to be answered include:

- What are the interfaces involved when SLM is the first process to become aware of a change to service requirements?
- How are the catalogue of services, SLAs and formal agreements affected?
- Who controls what decisions on SLA targets should they need to change?
- What impact will this have on the information security policy?
- Do those responsible for supplier management understand SLAs and other formal agreements?

One of the common effects of a change to business needs and service requirements is that the need for a new service is recognized, or that an existing service has to be substantially changed. The interface implications of this are described below.

Processes operated by other parties

There should be evidence that the interfaces to processes operated by other parties are defined and controlled. This type of service model has many names including outsourcing and out-tasking. Virtually all tasks operated by a supplier include operation of a process in the scope of the 20000 series, so this is obviously significant. A service provider cannot exclude requirements because they relate to a process operated by another party.

For processes operated by other parties it is particularly important to have clearly defined interfaces. Not only is this how the contribution made by the other parties is managed, it is necessary for audit evidence.

New or changed services

Part 1, Clause 5 includes requirements for new or changed services. The service provider does not have to plan, design, document or develop new or changed services. However, there should be an audit trail of such activities having been performed, with the service provider able to either accept or reject the output if it does not meet the agreed acceptance criteria.

If service providers are unaware of proposals for new or changed services until late in the process, they are unable to conform to the requirements for new or changed services. This is because there should be a link between any projects developing services and change management. This enables change management to have the opportunity to understand the potential impact of the change (or changes) and to reach a decision on acceptability. It should also be clear at which time control of decisions passes from those responsible for new and changes services to those responsible for change management under Clause 9.2.

Financial considerations

Budgeting and accounting are very dependent on information from other processes. No process is free, so all other processes are in turn also dependent on the information from financial management, even though some aspects of financial management are out of the scope of the 20000 series, for example charging for services.

Some of the greatest risks arise from a lack of understanding that financial management plays a key role in enabling a service provider to measure value for money of overall service management and of individual processes.

Most service management budgets rely heavily on asset and inventory records being accurate and up to date. For example, the number of PCs is related to the cost of support so if the records are out of date the budget for the cost of support will be wrong. This is also a nonconformity under the Part 1, Clause 4 requirement for control of assets, including software licences. This can also have legal implications.

Key point

An example of bad practice is service or workload information being provided too late for a budget cycle, meaning the budget is unrealistic. This can impact the ability to provide the service for the whole of the next budget year. It can have such a detrimental effect that it cannot be resolved in a single year and continues to impact the finances for much longer. The PDCA cycle could also accept or reject proposed options for continual improvements based on incorrect financial information. Plans for new services notified too late might not be achievable with the available funds, or in order to protect the customer's business, funds might have to be transferred from one activity to another.

Capacity and performance

Common failings include information not being provided to or from capacity management on non-technical resource requirements. Office accommodation, desks, basic facilities and the people that use them, are all resources that should be considered by capacity management. Loss of performance from inadequate staffing of a service desk can be just as damaging to a customer's business as a slow connection because of insufficient bandwidth. There is a close link between resource management in Part 1, Clause 4.4 and capacity and performance management.

Major loss of service

For service continuity a decision made for one process can have a serious impact on the service provider's ability to meet commitments in the event of a major loss of service. When changes are being considered it should be clear which process has responsibility for and control of the decision-making step.

A wide range of information is required for the planning of service continuity and then the subsequent testing of plans. If the service continuity plans are invoked and it is established they have been based on incomplete and therefore unreliable information, the result could be the inability to offer a workable service for many weeks after a major loss of service.

Availability management

In a very similar way to problem management, availability management can create the need for change or can be impacted by a change, especially a change that has failed. Table 5, showing interface definitions, illustrates the technique for documenting a process and its interfaces. Examples of tables showing inputs and outputs to a process are given for availability management in Tables 6 and 7.

Table 5 – Example interface definition

Input information	Source of input	Process	Output information	Output to
Supplier service report on major incident	Supplier and the service provider's supplier management	SLM	Impact statement on service	Customer, BRM and SLM
			Recommendations on implications for the contract	Supplier management
Customer's business plans	Customer and/or stakeholders	BRM	Implications of major changes on service and service levels	SLM
Implications of major changes on service and	BRM	SLM	Discussion document on proposed changes to the services, SLAs	BRM, customers, interested parties

service levels			and service catalogue	
Customer satisfaction feedback	Customer, stakeholders, end-users	BRM	Analysis of the strengths and weaknesses of the service	SLM
			Recommendations for improvements	PDCA improvement plans/service improvement

Table 6 – Example inputs for availability management

Input from	Information	ISO/IEC 20000 requirement
SLM	Availability requirements	The agreed requirements shall take into consideration applicable business plans, service requirements, SLAs and risks.
SLM	Availability requirements	The service provider shall create, implement and maintain an availability plan(s).
Change management	Request for impact assessment on availability management and availability plan	The service provider shall assess the impact of requests for change on the service continuity plan(s) and the availability plan(s).
Incident management	Incident data, major incidents and outages	Unplanned non-availability shall be investigated and necessary actions taken.
Problem management	Cause of incidents causing lost availability	

Table 7 – Example outputs from availability management

Output to	Information	ISO/IEC 20000 requirement
Service reporting	Availability metrics	Availability of services shall be monitored, the results recorded and compared with agreed targets.
Change management	Impact assessment of proposed changes on the availability plan	The service provider shall assess the impact of requests for change on the service continuity plan(s) and the availability plan(s).
A plan for improving the service	Changes to improve availability	Unplanned non-availability shall be investigated and necessary actions taken.
Change management	Proposed changes required for availability management	Unplanned non-availability shall be investigated and necessary actions taken.

Resolution processes

A common example of bad practice is the resolution processes not recording information or recording it inconsistently. This can provide a false basis for predicting the impact of a change to the service or the ability of problem management to identify a root cause. The workload information required for capacity management will be an underestimate and the performance of those following a process can fall below acceptable levels.

Configuration management

The service provider needs to define the interface between configuration management and financial asset accounting because financial management requires asset and cost information managed by configuration management.

Configuration management is a primary interface to update information about releases. When a release is deployed configuration information is updated. Release and deployment documentation includes information on enhancements and known errors, fixed or still present, in a release.

Change management

Unlike some of the other processes, change management has several compulsory interfaces to other processes. This is because the information passing to and from the process is essential for the effective management of changes. In most cases this is information flowing to change management. The outcome is a decision on acceptance or rejection of the request for a change. Processes such as problem management are likely to seek information on recent changes as part of the problem analysis.

Release and deployment management

Changes subject to Part 1, Clause 5 use the release and deployment management process. The release and deployment process works closely with change management on planning releases and deployments. Examples include: a release can contain many changes, each deployment of a release will be approved and controlled by the change management process, scheduled release and deployment dates will be on the change schedule.

Example – incident management by a supplier

The management of Company A's IT services department had outsourced the service desk function to a supplier, Company B. The supplier operates part of the incident and service request process.

The service provider, Company A's IT services department, needed incident management to be done to an exceptionally high standard. As a result the process and interfaces had to be defined so that:

- all incidents for the services and infrastructure are recorded;
- incident information is available for use by all those that require it, not just those involved in incident management;
- procedures to manage the impact of incidents are co-ordinated between the service desk supplier, Company B, and the service provider, Company A;
- the procedures that define the recording, prioritization, business impact, classification, updating, escalation, resolution and closure of incidents are aligned across organizational boundaries;
- personnel operating the process are highly trained in the way to handle incidents;
- all actions are recorded on the incident record;
- all personnel involved (first-, second- and third-line support groups) have access to information such as known errors, problem resolutions and the CMDB;

- Company A's customers are kept informed of the progress of their reported incident, by an agreed and understood process.

Information and management reports from the service desk provided by Company B need to be available to the second- and third-line support groups as service management cannot be effective without this. The contract between Company A and B was changed to allow Company A to have greater control over Company B's operation of incident management.

Chapter 6 'What does it mean for me?'

Introduction

When establishing or changing the SMS, a service provider should take into account that people have a strong desire to know 'what does it mean for me?' This chapter describes managing this circumstance.

For some people any change is a potential threat. They want reassurance that they will still have a role after the SMS has delivered the promised efficiency benefits. Each 'me' could potentially make or break the project that establishes the SMS if their need to know the way they will be affected is ignored. The 'me' in question includes everyone from top management to the most junior member of staff. Each 'me' will be affected differently by the SMS. Top management could be worried, although possibly they will hide it more effectively than junior personnel.

Top management will want to know the benefits in financial and service terms and will need reassurance that 'getting 20000' isn't just a gimmick. An ambitious manager will wonder if it will help with a promotion, or worry that involvement will risk their credibility. It is important to quantify the benefits, in order to reassure people that the changes are not introducing a bureaucratic overhead but are implementing better ways of working and delivering a service.

Leadership

Major change, such as establishing an SMS, is sometimes attempted without an understanding of how important it is that managers and personnel feel positive about the proposals. Proposals need to identify the way the changes affect what people do on a day-to-day basis. Very few people see changes as a positive experience, unless they themselves decide what the changes should be.

Plans fail when management neither communicate the benefits of changing nor recognize the need to tell individuals how they will be affected. The short-, medium- and long-term benefits for each involved or affected group or individual should be as tangible as possible.

One common failing is for technical training to be provided but process and procedure training to be neglected. If people do not know what to do and when to do it, processes and procedures will be followed inconsistently. An example might be something as simple as classifying incidents according to type under an incident management process and procedure. If personnel are not trained to do this properly the classification will be variable and the resulting information unreliable for service reporting or problem management. Before launching a project it is therefore advisable to ensure those involved understand what is to be done and why it is to be done. Plans should include development of suitable documents for training and long-term reference.

Where a service provider is a large organization, with a deep hierarchy of staff, based in a large number of separate locations, communications are difficult. Intentions at senior management levels dissipate as they cascade down the hierarchy, so that junior personnel do not hear anything at all or get a confused message.

When this is the case it is even more important that communication and cascading of management intentions are done well. This normally requires more positive action and resources than is normally required for a small organization where everyone knows each other and they all are located close together.

For all organizations the personnel should be well organized and co-ordinated and above all, motivated.

Agents of change

There are many advantages to a top-down approach combined with a safety net of bottom-up support from local enthusiasts acting as agents of change. It is important and part of good management practice to recognize the energy and influence of more junior management and practitioners.

Strong communities of enthusiasts cannot offset the effects of bad or non-existent leadership, but they can do much to redeem some of the failings of weak leadership. It is often junior enthusiasts that initiate new ideas and identify practical approaches because of their detailed understanding of day-to-day service. Once a sizeable community of best practice enthusiasts is established, management can no longer be vague or tentative with their statements and policies. Only a naive manager attempts to manage the scale of change required without the support and cooperation of more junior colleagues.

Table 8 – Needs and characteristics of motivated staff

Needs	Characteristics
• To have a challenging job that gives a sense of achievement, responsibility, growth, enjoyment and promising prospects for promotion • To have efforts recognized and appreciated by management, peers and customers • To have the trust and support of managers • To be able to use initiative and be allowed to complete tasks without being constantly supervised • To work in a team of people who are also motivated	• Energetic and full of initiative • Think for themselves • Appreciate recognition and challenges • Seek opportunities to improve their capabilities • Take proactive and positive actions to solve problems • Believe that their contribution can make a difference • Set their own challenging and achievable work targets

Providing the right people

The SMS, including the service management processes, will require the service provider to have personnel with appropriate education, training, skills and experience. The SMS will not be effective unless personnel are suitably skilled and motivated.

Action should be taken if the current practices are defective because there has been too little training in the past or because practices are currently acceptable, but should substantially change, for example to improve interfaces to other processes.

Setting objectives for individuals that will be involved or affected by change is important, e.g. increasing customer satisfaction, reducing downtime and risk.

Example – Setting the right objectives

There were many complaints about the time it took to get through to the service desk. Many users tried to contact other support groups directly. It was found that only 30% of calls were answered in six rings. No other measures were produced. To improve the call answer times, the service desk manager gave each member of the service desk a target of answering calls within six rings. This was supported by a bonus for each member of staff and led to 95% of calls answered in six rings, but the users continued to complain.

A review identified that there had been a change in working practices. In order to answer calls within six rings the staff were not logging all the calls. Also more calls were referred to other groups, instead of being resolved by the service desk. Analysis showed that if a call was not answered within the target of six rings it was not usually answered at all because picking up any call that had rung six times did not help achieve the bonus. The target and bonus had changed the service desk practices in a way that had been unintended.

The service desk staff and manager held a series of workshops. The result was a set of new targets suggested by the service desk staff themselves. These new targets included the original call answer times but were extended to cover maximum call pick up times as well. The new targets included measures on call fix rates and increased customer satisfaction with the service desk.

A bonus was split across individual performance, overall service desk performance and was tied to the new targets, including customer satisfaction. Within three months of the new targets being put in place the average call pick, answer and fix rates improved. No customer complaints were received at all and customer satisfaction was reported to be much higher.

Changing the organization

It can sometimes be necessary to change an organizational structure or correct a mismatch of roles, skills and personality types, in order to have a highly effective SMS. This is not because an SMS requires a certain type of organizational structure, but that an ineffective structure will make it very difficult to improve processes to an acceptable level.

The personality of individuals can make a difference, e.g. an effective member of a user facing group enjoys dealing with people and has an enthusiasm for customer service. A person who is only interested in technology can be very unhappy in a process management role and

function much more effectively in a back office role with much less interaction with users, and possibly even with their colleagues.

Roles and responsibilities

Service management roles, responsibilities and competences should be redefined and maintained as job requirements change. If this is done, staff will understand their role and the way they contribute to the overall service and service management processes. They are more likely to be motivated and effective than an individual who is left to operate in isolation, without understanding the way their role fits in with service management as a whole.

A simple method of keeping track of who does what is provided by a RACI matrix. RACI is an acronym for responsible, accountable, consulted and informed. An example is given in Table 9. This also shows who is responsible and has the authority and obligation to make decisions.

Table 9 – RACI matrix example (Level 1)

Task	Account-able	Responsi-ble	Consulted	In-formed
1. Log request for change (RFC)	Change initiator	Change initiator		
2. Categorize RFC	Change manager	Change manager	Configuration manager	
3. Assess, appraise and schedule RFC	Change manager	Change manager	Configuration manager	
4. Build, test and implement change	Implemen-tation manager	Implemen-tation manager	Change manager	Configu-ration man-ager
5. Verify and close	Change manager	Change manager	Configuration manager	

Who talks to whom?

There is a close link between understanding and documenting roles and responsibilities and keeping track of interfaces between people. This is particularly useful when the interfaces are across organizational boundaries.

Table 10 provides an illustration of one approach, often called contact maps. The row and column headings show which people (or roles) interface and the cell where the row and column meet shows the purpose of the interaction.

This illustration is based on an actual example in use in a large organization. It is not intended as a model for other organizations but simply to demonstrate the use of the technique of mapping interfaces between processes or people.

Chapter 7 Documentation and audit evidence

Introduction

This chapter describes the use of documents in managing the SMS, advice on their control and what the auditor will expect to see. Example audit evidence is included in Annex C.

Documents, including records, are used to ensure effective planning, operation and control of the SMS. Documents are also a very important part of providing evidence during an internal audit or certification audit, even though the 20000 series is intended to be about 'doing not documenting'.

The 20000 series treats records as a special type of document. Records show what has been done, not intentions. Control of records is similar to control of other types of documents and the Part 1 requirements are based on ISO 9001.

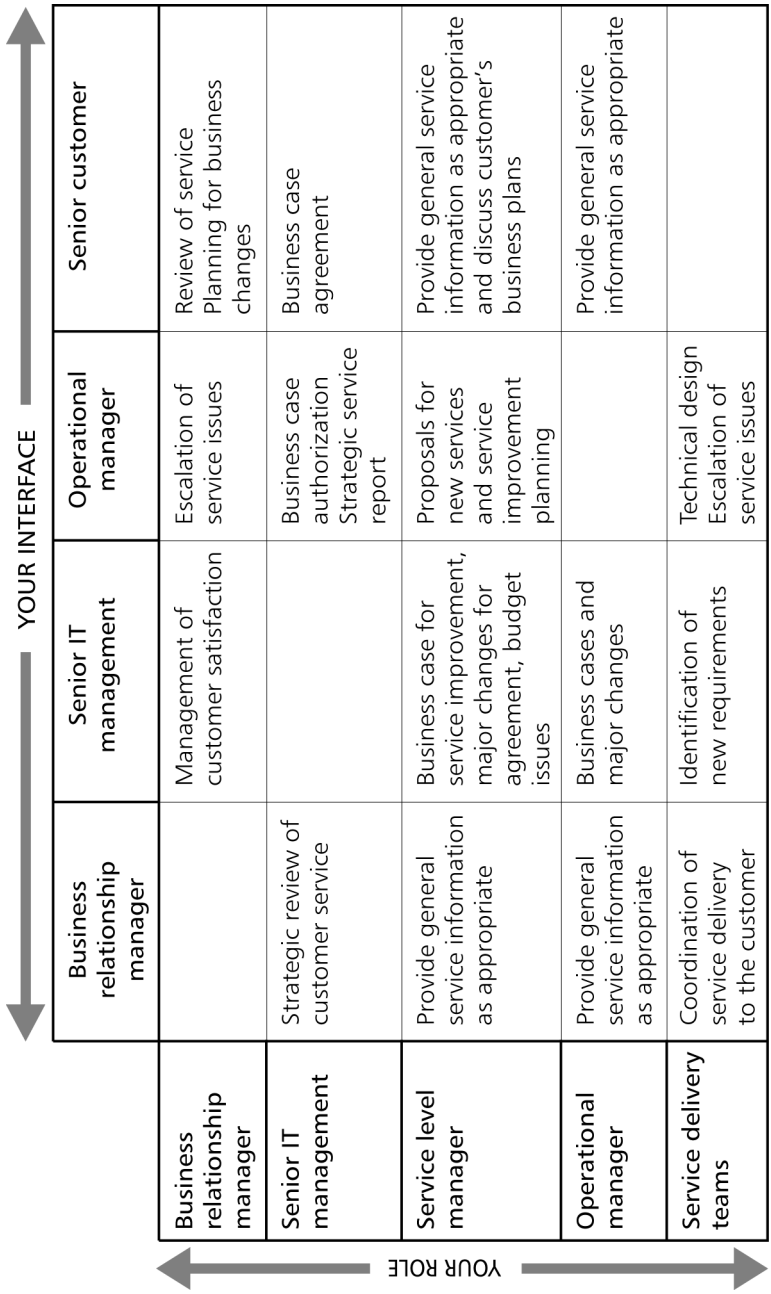
Example documents

All clauses in Part 1 involve some documents. The following examples need to be documented to meet the requirements of Part 1, Clause 4.3:

- policy and objectives for service management;
- service management plan;
- policies and plans created for specific processes required by Part 1;
- catalogue of services;
- SLAs;
- service management processes;
- procedures and records required by Part 1.

Other documents are always necessary for effective operation of the SMS and delivery of the services. Examples include documents and records from suppliers, including service reports, improvement plans and any contractual obligations. Other examples can be from the customer, including business plans and requests for new services.

Table 10 – An example of interface mapping



Authorities and responsibilities

Documents and records should be authorized at each stage, including production, review and agreement for them to be issued. It is bad practice for the person who creates a document to also review it and the person who reviews it is not normally the person who authorizes it.

Document control

Control of documents is via a set of controls documented in a procedure. This covers each stage of document production, issue, review and withdrawal:

- creation and approval of documents, before they are issued;
- announcements when new documents are available and what purpose they serve or when documents are withdrawn as obsolete;
- review of documents at suitable intervals to identify necessary changes;
- withdrawal or addition of a new document following the review;
- easy-to-use version control information: status, change history, roles such as document author and who authorized the document for issue;
- document control so that only the correct version is made available for use, old documents are removed or archived and draft documents are kept separate from the current document in use;
- formats, templates and software used to produce and control the documents so that they are usable after changes in software;
- document control information for documents of external origin.

Documents that are configuration items (CIs) are also managed by change management. Document review is essential to ensure that documents are fit for purpose, especially before they are agreed. Techniques such as peer group review can be very effective.

Record control

Most of the controls for documents apply to record control because records are a special type of document. Records, which are evidence of what has actually happened, can be subject to stricter security controls than other types of document, which describe intent. The service provider follows a procedure that ensures record identification, storage, protection, legibility, identification, retrieval, retention and disposal.

Retention and disposal

Records show what happened at a point in time, so when other records are produced later, the earlier records might need to be retained and not replaced. There can be a legal requirement to retain records, because they show what happened. The length of time is often determined by regulatory and statutory obligations, e.g. financial records, records on changes for Sarbanes-Oxley etc.

There can also be contractual requirements for retention of records, in some cases because the customer needs access to old records for their own statutory and regulatory obligations. The service provider's own organization should agree how long a record should be retained and build the retention period into a procedure. The procedures should include details of records that are disposed of, especially records that include information that should be kept confidential. The procedure should also state what is done to the record after the retention period.

Links to information security

It is sometimes appropriate to develop a policy on document and record control, to reinforce the importance of handling records of sensitive information. This links strongly to the requirements in Part 1, Clause 6.6, on information security. An information security policy can drive the Part 1, Clause 4.3 document and record management procedures.

Ease of use

The 20000 series makes no reference to any type of preferred format or media for documents. However, many service providers find that software for document control makes it much easier to meet the requirements in Part 1, Clause 4.3. There is less risk of losing or accidentally overwriting a document and many of the procedures can be automated.

Although an auditor is unlikely to critique the style of a document, the document will provide no value if it is difficult to understand, e.g. overly technical language for a non-technical reader.

Document libraries

Control is easier if there is a library for the documents and records. Defining the relationships between documents is simplified by:

- grouping related documents into a logical set, e.g. folders;
- referencing dependent documents in a document;

- defining the relationships between documents;
- change records using the configuration management records.

Some service providers include a table in the document control procedure that shows where each type of document and record is held physically or electronically.

Alternatively, or as a supplement, a graphical representation may be used, such as the example in Figure 5. This is a representation of the hierarchical relationships, with supporting details. In this example, the links joining the boxes represent hyperlinks if the documents are on an intranet, or manual cross references if not.

Checklist for documents and records

1. Use templates for documents
2. Use standard formats for each type of document
3. Identify, register and control external documents
4. Use unique document identification, registration and version control
5. Create documents for effective use by target audience
6. Track document status and changes to status
7. Use change management for documents
8. Verify document to check that it has the right scope and is fit for purpose
9. Review and approve documents before issue or re-issue
10. Provide secure backup for documents and protect against damage
11. Apply appropriate security to protect against unauthorized use
12. Select suitable media and format for the target audience
13. Agree policy, process and procedure on withdrawal and archiving
14. Agree policy, process and procedure for return of external documents
15. Agree policy, process and procedure for secure disposal

What will the auditor want to see?

The answer, at least in part, is 'It depends'. Most of the audit evidence of the effectiveness of the SMS, including the service management processes, is based on documents, including records. However, there is no list of audit evidence in Part 1.

An auditor will ask to see documents and records appropriate to whichever Part 1 clause is being audited. If the audit follows a previous audit it is likely that the auditor will ask to see documents that relate to a previously noted non-conformity. For example, an auditor can start with the documents on a change to the customer's business that led to a

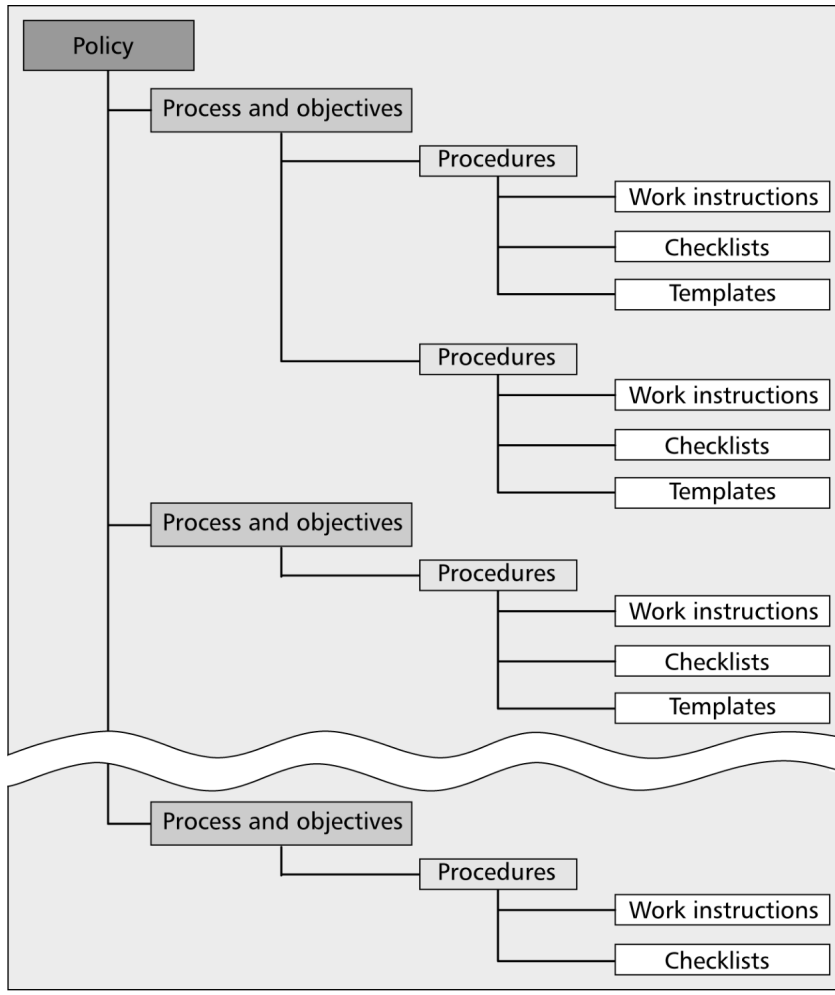


Figure 5 – Example hierarchical document library

change to the service and the service provider's SMS. The auditor can then ask for the evidence that tracks this change rippling through the processes involved. This includes those in the supply chain of BRM, SLM and supplier management.

Other documents that the auditor can check are the change management records providing evidence that the technical, resource and personnel changes were considered. For higher risk changes, the planning for new or changed services from design onwards could be audited.

Key point

Auditors will expect documents and records to be grouped in an orderly structure, providing evidence of a logical approach to document and record management. Auditors will also expect people to be able to find documents easily. Auditors will expect people to be able to identify and explain the documents and records that they use to support their service management activities.

Documents, including records, are used to ensure effective planning, operation and control of the SMS. Documentation needs to be designed and written to fulfil the purpose of the document and the target audience. It is relatively easy for an auditor to see if people have difficulty finding and using documentation.

Example – Documenting not doing – too much of a good thing

A service provider was confident that the service delivered was good, but top management were concerned that it would not be possible to prove this to an auditor because there were few documents as evidence. A project to fill in all the gaps produced many documents. However, despite all the effort, there were problems with the quality and quantity of documents.

- Many new documents had no identification and versioning.
- Documents were very long and extremely detailed.
- The documents titled 'Policy' included covered processes and procedures.
- Personnel could not understand the logic of the document index.
- The search facility produced unexpected documents.

A new manager established a document library structure, document management policies, and templates. Some documents were reused but reduced in length. Policies were less than one page and processes a maximum of two pages. The document control information was a single page at the end. All documents were under the control of a web-enabled document indexing and search facility. Personnel were able to locate useful information quickly.

This encouraged them to adopt a consistent approach to their work, improving service management and reduced the risk of the wrong document being used.

Chapter 8 Service reports

Introduction

This chapter describes the principles of good service reports, the way the Part 1 requirements can be met and advice on good practices.

Part 1, Clause 6.2, service reporting, is one of the shortest in Part 1. Despite its brevity it is important to an effective SMS. Clause 6.2 covers all service reports, and is not limited to those produced for the customers and users. Service reports are a mechanism for integrating processes, the basis for reviews and internal audits and are a high proportion of the evidence for an audit.

What is a service report?

A service report can be a list, table or chart. Although a picture is said to paint a thousand words, most charts require supporting text, so that the combination of the two is more effective. For some organizations, tables will be preferred to charts and for some, the reverse. Each service provider should decide what is most appropriate for each target audience and the information being reported.

The principles of good service reports

Key point

> A common fault in service management is reports that contain simply what has been historically available, produced by habit, and never stopped, no longer relevant or not what is needed. The 20000 series provides requirements and advice on making service reports an effective part of an SMS.

A good service report is one that illustrates the speed, effectiveness and predictability of processes or services. A good service report therefore

shows how well an SMS has been designed and implemented and policies or objectives achieved. A good service report is timely, clear, reliable, concise and appropriate to the recipient's needs. It is sufficiently accurate for decision-making. Good service reports contain information that is easy to assimilate and allow the reader to identify what actions to take. Conversely, a bad service report is based on inaccurate data, difficult to understand, implies greater accuracy than is possible, covers unimportant topics or those that cannot be changed.

Good service reports are not an accident. The service reporting process has to be designed just like any other in the SMS. The design starts with an understanding of the service management policies, objectives and the relationship of service reporting to the rest of the SMS. Reports suitable when an SMS was implemented can become unsuitable as changes are made to the SMS, the service or if there is a change in the customer's business activities.

Service reports should focus on those things that matter and those that can be changed by the service provider. Service reporting also has to take into account limits on what can be reported, e.g. accuracy of the data or manual effort to produce the service reports. The availability of tools can be a limitation.

Key point

Accuracy and precision – don't let the numbers fool you

Service management measures, such as availability, are often reported to several decimal places, but in many cases the value is based on manual entry of start and end times for incidents, often rounded to the nearest five minutes. The resolution time can be wrong by much more than five minutes even if the start time is correct. For a short incident this can represent a sizeable percentage error. Changes over time can be due to errors in the underlying data or changes in how the data is collected. This is often an unintended consequence of assuming automating report production means reports are accurate.

Service reports are used as information flows between processes and are therefore part of process integration. Examples include information on lost availability or capacity issues used by BRM during meetings with customers.

The information in service reports that passes between processes and across a supply chain can be used to assess how well the interfaces are managed. For example, service reports on changes passing to problem management, and vice versa can be checked during an audit.

A checklist is also given below.

Checklist for service report design

1. Who should receive a report and why?
2. What does the target audience need to know and why?
3. What format would the audience prefer to receive?
4. Will the frequency of the report be appropriate?
5. Is the cost of the metric production justified?
6. Are supporting metrics available if required?
7. Is it clear what process(es) underpins each report?
8. Is the relationship to other metrics understood?
9. Is the source of the data and its accuracy understood?
10. Are the algorithms understood and documented?
11. Is the data accurate enough for the intended use?
12. Are the reports given greater precision than the accuracy justifies?
13. Is the link between objectives and critical success factors clear?
14. What action will be triggered by the reports?
15. Are the contents suitable for informed decision-making?
16. Does this metric report on something where no action is possible?
17. Who interprets the metric and will they be able to do this accurately?
18. Is the interpretation objective?
19. Will the information be understandable to the recipient?
20. How will the metric and service reports be tested?
21. Have you scheduled periodic reviews to make sure the reports are still required?
22. Is report design under the control of change management?

Minimum requirements

Part 1 requires the following minimum reports to be produced:

- performance against service targets/failure to meet service requirements;
- information on major incidents,
- reports on deployment of new or changed services;
- invocation of the service continuity plan;
- workload characteristics including volumes and periodic changes;
- nonconformities against Part 1, i.e. the requirements for the SMS;

- trend information;
- customer satisfaction measurements;
- number of complaints and analysis of the reasons for complaints.

The service provider is also required to use the reports for decision-making. This could include use in a service review as part of SLM, or a management review as part of Part 1, Clause 4 requirements. Evidence of actions taken can be checked by the auditor. This may also be checked during the management review under the PDCA cycle. Agreed actions should be communicated to interested parties.

Other parties and service reports

Part 1 includes requirements for information about the service provided by other parties. Under the requirements of Part 1, Clause 4.2 service reports are essential for demonstrating governance of processes operated by suppliers, lead suppliers, internal groups and customers acting as suppliers.

Service reports should reflect the relationships between the service provider and other parties. For example, if several sub-contracted suppliers are managed by a single lead supplier, the lead supplier should report on the whole of the service they provide, including any services or service components provided by sub-contracted suppliers.

Types of service report

Reactive

Reactive reports show what has happened, particularly from the predominantly reactive processes, such as incident management. They include:

- service desk telephone call volumes per month;
- numbers of problems and incidents;
- security incidents;
- number of changes;
- response times.

Value is added to these basic reports listed by producing them for each service, customer or location etc. They can also be subdivided or ordered by categories such as type of incident, problem or change, scale of impact or priority.

These are the easiest reports to produce in the early stages of an SMS. However, they can be seen as only reporting bad news, i.e. what went wrong, without any information on what went right or corrective action to prevent repeat failures.

Proactive

Proactive reports give advance warning of events that could impact the service. This type of report is frequently based on the extrapolation of historic information. Proactive reports can be predictions based on the estimated impact of expected events, such as workload increases from a new product launch. If acted upon within the right timescale, they will enable preventive action to be identified and taken before the service has been impacted. As a result they can be harder to produce but will be more constructive to use.

An example of a proactive service report is given in Figure 6. This shows a combination of actual data monitored month by month for 13 months, trends and the maximum number of web page impressions predicted for the available capacity.

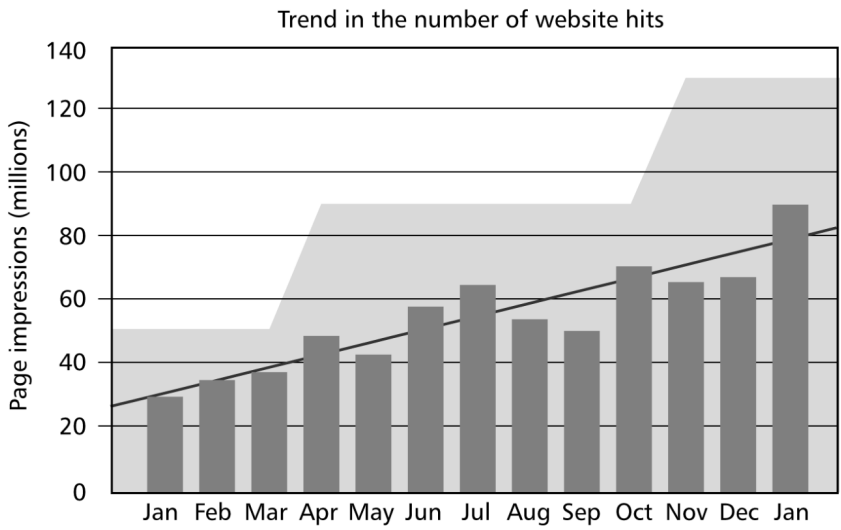


Figure 6 – A sample proactive report on website hits

Forward schedule reports

Forward schedule reports show planned activities, i.e. those activities that are predictable, intentional and usually desirable. Most are part of a change lifecycle and many are the result of projects. Examples include Gantt charts, change or capacity management reports. Giving notice of intentions via this type of report allows other people and processes to adapt day-to-day activities, if necessary.

Key point

All three types of report can be exception reports, i.e. only produced under specific conditions, e.g. a service outside agreed limits. An exception report is often appropriate to explain an unusual event that has either impacted the customer's service or put it at risk, such as a serious information security incident. Exception reports also reduce the number of reports routinely issued that actually report nothing of interest to the target audience. The definition of 'exception' should be agreed by the target audience.

Target audience

Reports should be designed for a specific target audience and not issued indiscriminately to anyone and everyone. A service report from one process should be designed on the basis that the target audience may be another process as well as those that are operating the process.

Under some circumstances the same type of report can be used by both customer and service provider, but with different objectives. For example, a report can be based on the number of 'How do I…?' queries, and be used to identify training needs, develop 'frequently asked questions' or used to assess the effectiveness of release and deployment.

Customer and user reports

Service reports for customers and users have an external business focus and should use the customer's terms and language, not the service provider's technical language or jargon.

Key point

Reports for customers should help the reader answer the following major service-related questions.

- Is the service delivering what the customer expects?
- Is the service meeting the customer's business needs?
- Is the service value for money?
- Has the service got better or worse?
- What can be done to improve what the customer sees?
- What can be done to improve the service delivered to the customer?

Customers should have reports that state the business impact/cost, not on the service provider's internal issues, e.g. trends in urgent problems that have been fixed by individual support teams. Customer reports are often linked to an SLA and will typically include information such as problems with system x, delayed billing for y days, with loss of z.

Service provider's reports

The service provider's own reports are intentionally internally focused and usually more numerous than those for the customer. The service provider's reports should cover the requirements of Part 1, Clause 4 for management responsibilities, continual improvements and process integration. These include:

- progress in establishing the service management policies;
- progress with communicating objectives;
- status and plans for service management documentation;
- progress with the definition of roles and responsibilities;
- training records against planned and budgeted targets;
- efficiency of the process, e.g. unit cost of a task;
- success of plans for improvements to the SMS.

Reporting on a policy is illustrated in the example below.

Example – Service improvement policy implementation

If a service provider's policy includes 'service improvements will be targeted at delivering a faster and cheaper resolution service', then a suitable service report could cover:

- trends in incident and problem volumes for problem avoidance;

- trends in average resolution times for faster methods of resolution;
- trends in unit cost of incident resolution to target cheaper unit costs.

These service reports are from several processes. In this example, the processes are incident and problem, IT budgeting and accounting.

A service provider has responsibility for the whole service that is delivered to the customer, and therefore needs reports that cover the whole service. The service provider should include service reporting needs when specifying the service they require from their suppliers.

Service providers will find it beneficial if their suppliers adhere to the same design principles when developing reports. This will ensure that the supplier's service reports, which are required to manage the interfaces between processes (and the whole supply chain), are compatible with those of the service provider.

The service reports should also cover components of the service and the service management processes. They typically cover the identification of underlying faults and workload or performance data. They reflect the components of the service, e.g. components such as servers, routers, hubs and cabling. They can include a low level of detail.

The terminology used and the overall view of the service will be from the service provider's perspective and can be much more technical than the reports produced for customers.

The reports should help to identify:

- service trends;
- unreliable components of the infrastructure;
- resource/cost intensive tasks;
- potential improvements.

Managing service reports

It is necessary to apply the principles of best practice document management to service reports, as described in Chapter 7.

Key point

The minimum information for each report is:

- identity, usually as reference for coding;
- purpose, what it shows and why it is produced;
- target audience, who should receive it and the way they will use it;
- frequency and timetable – when is it issued;
- data sources and any limits on or risks to accuracy;
- algorithms used.

This is expanded on in Table 11.

Table 11 – information about service reports

Item	Purpose/description	Example
Reference:	Code so that each report can be referenced unambiguously and easily controlled. Coding that groups similar types is useful, i.e. by policy or process. The coding should reflect hierarchical relationships between reports.	SLM-M-SLA-006 • SLM – process • M – monthly • SLA - report for customers • 006 – unique reference within this category
Name:	Simplifies discussions during the design and production of reports.	SLA report for [service name], MM YY
Target audience:	Role, function, department, organization level.	• Customer • Process owner for SLM • Process owner for BRM • Service manager Note: names of individuals go out of date too quickly and should not be used.
Objective/ purpose:	Why this report is produced, briefly defined.	Comparison with SLA targets, part of the commitment to the customer.
Links/cross references:	Identification of relationship between the report and the component of the SMS to which it relates. Some reports will have more than one cross reference. These linkages/cross references are similar to those in configuration management and are why service reports can benefit from being classed as CIs.	Service catalogue reference

Process interfaces:	What processes provide input information required by this report and what process uses this report.	Information from problem management used to link to change management, and vice versa.
Algorithms:	The way the report data are calculated. Should be published in an accessible glossary, or as part of the report.	
Data source(s):	For example, an automated monitoring system or manual logging. It is advisable to include the field names and a description of the data in each field used and not just the name of the system from which the data is retrieved. This ensures continuity in what is in the report.	The XYZ system, [field name1], [field name2], [field name3]
Target/control limits:	This is a trend or benchmark value: the service provider may choose to build in control limits, trends or an established industry benchmark. It should also be noted if a report is only triggered for issue when the actual value is outside agreed limits.	A target, such as a '95% fix time in eight hours', is common for service reports for SLAs.
Limits on accuracy:	Used to give context to the use of the information, i.e. avoid actions based on trends that are changes to logging practices etc. Notes on reasons for errors are useful.	Ranges, such as +/-X%. Accuracy is limited by errors from manual data entry of the start and end of events.
Issue date:	Issue dates do not need to be actual dates, but relative timings.	'x days after month end'
Check date:	Could be used to establish when the continuing production of the report should be reviewed.	End of financial year

Chapter 9 Service supply chains

Introduction

This chapter explains the three processes: supplier management, service level management (SLM) and business relationship management (BRM). It explains the way they each act as part of a supply chain for delivering services.

A service supply chain affects the definition of scope and the establishment of an SMS. It also always spans the three processes: BRM, SLM and supplier management. Due to the nature of service supply chains the three processes are particularly closely related and are strongly interdependent. However, each process has different objectives, and a different focus.

Example supply chain

The three processes always cross organizational boundaries. The boundaries are:

- supplier management interfaces to suppliers and lead suppliers;
- SLM interfaces to the customer, BRM and supplier management;
- BRM interfaces to the customer;

An example of a simple service supply chain is given in Part 1, Clause 7.2. This Part 1 figure is used as the basis of the figure below.

SLM is used to manage catalogues, SLAs, services etc. Figure 7 shows that BRM manages the relationship with customers. Customers interface to other service management processes, especially SLM. Suppliers are managed by supplier management. All three processes are in the scope of the SMS.

The service provider does not manage the sub-contracted suppliers. Lead suppliers are responsible for the management of sub-contracted suppliers, so the process for managing sub-contracted suppliers is outside the scope of the SMS. This is the case, despite the Part 1 requirement that service providers verify that lead suppliers are managing their sub-contracted suppliers to fulfil contractual obligations.

The service provider can be asked for evidence that they ensure the lead suppliers are managing sub-contracted suppliers, although the lead supplier will not be audited.

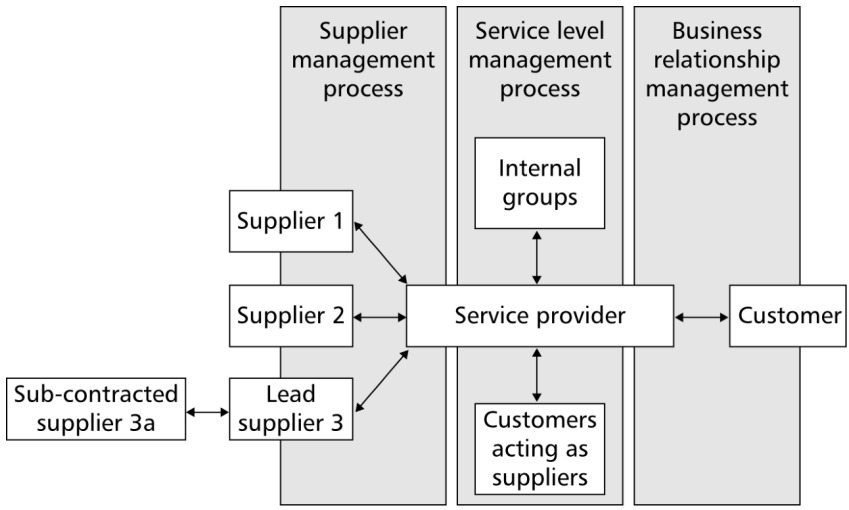


Figure 7 – A service supply chain

In Figure 7, two groups have been added: internal groups and customers acting as suppliers. Part 1, Clause 4.2 requires that both types of group are managed using SLM when the groups are providing part of the service by operating a process in Clauses 5 to 9.

The internal groups and customers acting as suppliers are outside the direct control of the service provider and scope of the SMS, but their *contribution* is within the scope of the SMS. This requires careful co-ordination and, at times, a great deal of diplomacy.

The three processes are all subject to control and improvement under the PDCA cycle. However, under Part 1, Clause 4.2, processes in Part 1, Clauses 5 to 9 may be operated by other parties. The involvement of other parties has a particular relevance for this service supply chain.

No matter how complex a service supply chain, the service provider is always responsible to their customer for the quality and cost-effectiveness of the whole service. This is irrespective of which parts of the service they deliver directly and which they receive from a supplier.

Table 12 shows a comparison of who is involved in each process and gives example reports and key measures for each party.

Table 12 – Comparison of the three processes

Part 1, Clause 6.1, SLM		
Who is involved?	Example documentation	Example measures/controls
Customer Service provider's service level manager	SLAs Formal agreements with internal groups or customers acting as suppliers. Service catalogue Service performance reports	Number and percentage of services that meet service level targets Variation of actual spend against budget for each service (link to financial management)
Part 1, Clause 7.1, BRM		
Who is involved?	Example documentation	Example measures/controls
Customer and interested parties Service provider's business relationship manager	Business strategy (if available) Service provider strategy and plans	Customer satisfaction that the services are aligned with the service requirements Customer approval of strategic changes
Part 1, Clause 7.2, supplier management		
Who is involved?	Example documentation	Example measures/controls
Service provider's supplier manager and contract manager (may be same person) Supplier's representative	Supplier contract SLA(s), possibly as contract schedules	Sign off by the service provider that the supplier's services are aligned with the business needs Number and percentage of contracts renewed

Reviews

Reviews are a feature common to all three processes described in this chapter. These reviews have some features in common but all three have differences.

- **BRM** is focused on customer satisfaction and future service requirements arising from changes to customer activities or priorities, including managing any complaints.
- **SLM** is focused more on day-to-day operational service issues, including the totality of the end-to-end service, but also considers service trends, particularly where a service target is at risk. SLM also includes reviews of the performance of internal groups and customers acting as suppliers that provide part of the service.
- **Supplier management** is focused on contract/performance management to ensure the supplier delivers the required service.

The PDCA cycle may also identify a defect in any one of the processes either as part of an internal audit or management review.

A service provider, particularly smaller in-house organizations, may hold the review required for SLM and BRM as a single meeting between the service provider and customer. Smaller organizations often have the same individual responsible for both SLM and BRM.

It is less common for supplier management review meetings to include the service provider's customer. This is because the service provider is responsible for the supplier's services and should be able to deal with any concerns, plans or queries relating to the supplier's services.

Business relationship management

BRM has the objective of establishing and maintaining a good relationship between the service provider and the customer, based on understanding the customer, its business drivers, plans and likely future service requirements. The customer's service requirements are shaped by their current and future business activities and the service requirements in turn shape the service management plan, via BRM.

The features of BRM are summarized in Table 13.

Table 13 – Key features of BRM

What to do?	Why do it?
Understand the customer's organization including users and other stakeholders	Develop a good relationship, anticipate what is required, who to talk to when
Understand the customer's business, plans and changes to business or service needs	Plan ahead for changes to requirements, plans, contracts and the rest of the SMS

Ensure there is effective management of the contract or similar formal documented agreement	See the full picture for the SMS, ensure the supply chain is optimized, get value for money from suppliers and be able to put process governance in place
Provide input to SLM on changes to business activity and services that require changes to SLAs	Update the service catalogue, SLAs, affected formal agreements or contracts and service reports. Contracts can take a particularly long time to change
Ensure complaints are handled effectively	Avoid a crisis building from a failure to take complaints seriously. Learn how to do things better in the future and provide input to the PDCA cycle for continual improvement
Ensure customer satisfaction is measured and managed and that a named individual is responsible	Understand what the customer cares about most, the strengths and weaknesses of the service, the way to build on strengths and to prevent a minor issue becoming a complaint
Provide input to a plan for improving the service	Help ensure that changes are planned and orderly, minimizing the risk and costs of changes

BRM plays a role in aligning the customer's business strategy and the IT strategy and, in turn, aligning the services delivered by the service provider to the business and IT strategy. Effective BRM requires a good understanding of the customer's business, the customer's concerns and the way the service affects the customer's business activities. The development of a good relationship should not be left to chance but should be planned. Although the service provider may operate commercially there are no requirements for identifying leads, qualifying a prospective sale or negotiation of charges.

Formal agreements or contracts?

SLAs may form part of a contract between the service provider and customer, usually as a schedule (annex) or possibly outside the contract but referenced from it. The main body of a contract normally takes legal precedence over SLAs. Despite the precedence of the main body, an audit will normally disregard any part of the contract that does not have a direct bearing on the SLA.

Part 1 does not require a legally binding contract to be in place between the service provider and customer, although there should be at least one SLA. For example, where the service provider and customer are part of

the same legal entity a legally binding contract is not possible. In these circumstances an SLA is essential and can be treated as if it were contractual.

Understanding the customer's needs

BRM includes a requirement that the service provider remains aware of the business needs and major changes that are being planned by the customer. The information obtained also forms important input to SLM.

Understanding the customer includes measuring the customer's satisfaction with the service. Perceptions can be shaped by whether or not the service meets the customer's business needs and is considered to be good value for money. The way the service provider reacts when the customer needs different services can also have an impact.

One of the challenges that service providers face is understanding the customer's service requirements. Other challenges include understanding the roles, responsibilities, accountabilities and authority levels of individuals in the customer's organization. Common methods of documenting interested parties include contact maps. These show the way the management structure of the service provider and the customers align, i.e. how each manager relates to their counterpart in the other organizations. Responsibility matrices may also be used.

BRM also identifies the interested parties who are likely to influence the services requested. For example, final decisions by a customer can be made by their procurement or finance department following consultation with interested parties.

New or changed services

New or changed service requirements are normally initially identified by BRM. BRM co-ordinates with SLM for changes to SLAs.

New or changed services are managed by the process in Part 1, Clause 5 if they represent a substantial change or risk to the service. This process interfaces to change management and via change management to release and deployment management. This kind of change can also cascade through and affect many other processes, including service reporting, service continuity and even the scope of the SMS.

This kind of change often triggers updates to the service reports, catalogue of service, SLAs, formal agreements with other parties, contracts with suppliers, as well as the agreement between the service provider and customer.

Complaints and customer satisfaction

Customer satisfaction is central to BRM. Satisfaction measurement is linked to the customer's perception of a service, the technology used and its perception of the people that deliver that service. Satisfaction measurements are also one of the links between BRM and SLM.

Part 1 does not specify the way customer satisfaction should be measured. Feedback may be qualitative or quantitative, obtained from only senior management in the customer's organization or from many users. An auditor will expect to see evidence that the approach used is suitable to deliver the information needed for improvement to be identified.

Part 1, Clause 7.1 requirements include a complaints procedure. It is important to be realistic and expect that at some time a customer will wish to make a serious complaint. This can be because escalation of a concern has failed, because a problem appears overwhelming to the customer or there is a crisis requiring exceptional action.

This requires a service complaint to be defined in advance of the procedure being invoked. The procedure should ensure that all complaints are recorded and managed until closed. There should be a mechanism for handling complaints that are not resolved.

Measuring satisfaction and managing complaints can identify risks to the relationship in time for the risks to be managed before serious damage has been done. For example, a gap opening between the SLA and the service the customer's needs will trigger low satisfaction ratings.

Checklist: Complaints

What constitutes a formal service complaint?

Is there ambiguity on what is and is not a formal service complaint?

Is the definition of a complaint so broad minor issues will be raised using the complaints process, undermining its effectiveness?

Who may raise a complaint?

Part 1 requires that it is clear who can and who cannot raise a complaint. Less serious issues are handled by escalation. It is common for the authority to raise formal complaints to be restricted to more senior management in the customer's organization, preventing abuse of the procedure.

Who should receive the complaint?

It is not normally advisable to rely on a single named individual being present to receive and act on a complaint, as the individual will not always be available.

Managers who receive complaints should be aware of the process so that they can ensure the process is followed and that the complaint is properly resolved.

How is the complaint raised and recorded?

The method of raising a complaint should be simple and effective.

Basic information on the person making the complaint is required, in addition to the details of the complaint. Recording should support analysis of the reasons for the complaint, tracking progress to resolution and closure.

If it is a recurrence of a previous complaint or is a repeating problem this information should also be collected, if possible.

Success criteria for resolving a complaint

The service provider should make sure the person complaining understands the next steps and the timetable of events. The service provider needs a process by which it can be agreed that the complaint has been resolved and the record can be closed. There should be unambiguous criteria for resolving the complaint, e.g. that a problem will be resolved by an agreed date.

Escalation of the complaint

There should be a clear route for complaint escalation.

Input to the PDCA/improvement cycle

At intervals, or after a very serious complaint, the nature of the complaints received should be analysed (under the PDCA cycle of improvements and input to service improvement plans).

The service provider should appoint an individual who is responsible for managing the customer relationship and measuring and managing customer satisfaction. Someone should also have responsibility for the quality of BRM. Some service providers allocate both responsibilities to the same individual. This role will vary depending on the nature of the service and the customer's organization. For example, services delivered to a single organization, even a very large one, will involve a high level of contact between the manager responsible for BRM and the customers.

Where the service provider is delivering a service shared by many customers, e.g. cloud computing and access to the Internet at household level, the BRM manager is unlikely to have much contact with the customers, but is still responsible for their satisfaction and any complaints.

Service level management

SLM is the link between the management of suppliers and the management of the business relationship with customers. Because of this, SLM can be a supply chain's greatest strength or greatest weakness.

SLM is also the vehicle for how internal groups and customers acting as suppliers are managed by the service provider, under Part 1, Clause 4.2.

SLM is focused on fulfilling service requirements based on records of services, service level targets and the characteristics of the workload. SLM is fundamental to achieving a balance between cost, quality and workloads. It establishes an understanding of the responsibilities of the service provider and of the customers, sometimes by negotiation and then formal agreement of an SLA.

Key point

Both BRM and SLM are required to hold reviews with the customer, for SLM this is focused on review of services and SLAs. Changes to the service requirements, catalogue of services, SLAs and other documented agreements should be controlled by change management.

If the customer develops ideas on new or changed services that are impractical or perhaps technically impossible, SLM can identify alternative ways of helping the customer meet their business needs. This requires access to a broad base of technical experts and information, including the likely costs of the new or changed service.

Service level management documentation

The relationship between SLAs, a catalogue of services, formal agreements between the service provider and other groups, contracts with suppliers, service management plans, service reports and training plans is shown in Figure 8.

Part 1 includes a requirement that the full range of services provided, plus the corresponding targets and workload characteristics are agreed and documented by the service provider and customer in a catalogue of services.

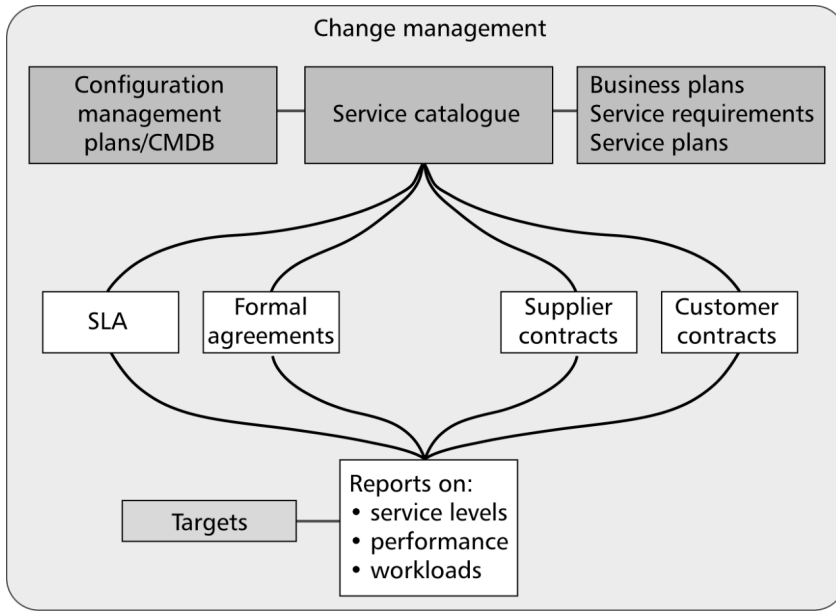


Figure 8 – Relationship between documents in the supply chain

The catalogue of services holds information that defines the available services including information common to all SLAs, such as:

- the SLA change control mechanism;
- glossary of terms;
- targets common to many SLAs.

A well-designed catalogue of services creates a shared understanding of the services. Using a catalogue means that SLAs do not have to be repetitive with the same text in each SLA. The SLA can refer out to a catalogue where the text is held only once. This has the benefit of simplifying version control of the SLAs as standard text needs only to be updated once, reducing the risk of SLAs being accidentally out of step.

If catalogues and SLAs are held online the information is readily available to the service provider, the customers, users and the auditor, although Part 1 does not specify the medium to be used for these documents.

It is best to base the catalogue on the customer's view of the services. An auditor can check that a repository such as a catalogue exists. The auditor will also check that the services are defined in a well-designed, accessible manner, with the repository kept up to date and written from the customer's viewpoint.

Service level agreements

A service level agreement (SLA) is a written agreement between a service provider and a customer that documents services and agreed service levels. The SLA should be based on service requirements, which in turn should be based on business needs and budget.

Too many targets in an SLA can create confusion and lead to excessive overheads but any targets that are included should be defined from a customer perspective. Some service providers set a limit of no more than five targets per service. Before the SLA is agreed the service provider should be confident that it is possible to report on the services in the SLA from the customer's perspective, using terms that the customer understands.

Best practice SLAs are based on understanding not only the service provider's commitments, but also the role of the suppliers, customers and users. This should include the impact they each can have on the service and the service provider's ability to meet their commitments.

SLM works very closely with BRM on changes to SLAs made by SLM. SLM should seek information from BRM on the customers, their organizational structure, culture and levels of customer satisfaction (and causes of dissatisfaction) and any changes to service requirements that emerge.

The SLAs are usually supported by contracts between the service provider and suppliers. Other supporting documents are formal agreements between service provider and internal groups within the same organization as the service provider. In some cases this is the 'customer will act as a supplier'.

Reviews of services and SLAs

Part 1 specifies that reviews should occur 'at planned intervals'. The choice of an acceptable planned interval should be influenced by the rate of change to the customer's service requirements, and any changes the service provider plans that could affect the service. The phrase 'planned intervals' leaves more of the burden on the service provider to prove the intervals are suitable than 'at least annually'.

A review should be effective and efficient and an auditor will expect to see an understanding of:

- the customer's service requirements;
- the importance of preparation by the service provider;
- the effective use of service reports;
- the need for information on planned changes;
- feedback on implemented changes;
- the purpose and importance of taking minutes and documenting actions.

The auditor will expect to see that minutes are sent out in a timely manner and actions are followed through.

Supplier management

Supplier management ensures that there is a seamless service, where the service provider takes overall responsibility for the service. Under this model the customers do not have to be concerned about who does what.

A lead supplier is required to act as the interface between sub-contracted suppliers and the service provider, providing a seamless service. Lead suppliers should be able to demonstrate that sub-contractors also meet contractual requirements.

The selection of suppliers or procurement of services is excluded from Part 1 requirements. However, there are benefits from BRM, SLM and supplier management being involved in procurement, if only to avoid an unacceptable result from the procurement process.

Key point

For contract management:'… the service provider shall have a designated individual who is responsible for managing the relationship, the contract and performance of the supplier'. This could be reflected in a policy that requires there to be a contract manager, specifies what type of person should be appointed as a contract manager, and includes a high-level view of what the role should achieve.

Supplier management ensures that appropriate services are agreed with suppliers and that the suppliers deliver the service they have been asked to deliver in the way they have been asked to deliver it. If the services

are out of alignment the service provider is unlikely to be able to deliver the service agreed with their customer, or do so only at an unacceptable cost. For example, agreeing service commitments with a supplier, such as the time taken to respond to requests, that is slower than the time agreed with the customer will mean the service provider is unlikely to meet their targets.

Key point

Alignment of service commitments: 'The service provider shall agree with the supplier service levels to support and align with the SLAs between the service provider and the customer.' This could be reflected as a policy on SLAs covering both supplier management and SLM. The policy could state that there should be alignment of services along the supply chain of 'supplier – service provider – customer', and the way that alignment should operate. As organizations can have signed long-term contracts with suppliers that are not aligned with the customer's needs, the policy could also extend to cover interim arrangements or a transition to new and more appropriate arrangements.

Policy, process and procedure are not normally included in contracts, but may be referred to as part of a quality manual, service management plan or similar document set that is referenced from the service requirements.

During an audit, service providers should demonstrate they are able to control the processes. As supplier management crosses boundaries to external organizations, it can play a particularly important part in the way the service provider demonstrates this control. This includes demonstrating that the governance of processes is included in the contract between the service provider and supplier. For example, the contract should define the way improvements to the processes and services will be prioritized and managed.

Service providers should behave as responsible customers towards their suppliers, if they themselves are to meet the requirements for supplier management, e.g. by attending reviews with the supplier.

The supplier is not required to fulfil the requirements of Part 1 in order for the service provider to do so, but the full benefits will only be obtained if the supplier and the service provider follow processes that are aligned. Service catalogues, SLAs, service reporting and the PDCA cycle are as beneficial to the supplier as they are to the service provider. The

supplier's performance against service targets should be monitored and reviewed, with any required improvements being input to a plan for improving the service.

The following is a summary of the requirements for supplier management.

- Ensure there is a contract and contract manager for each supplier.
- Agree business, service and communications requirements to be provided by each supplier as SLAs or other documents.
- Ensure the roles, responsibilities and interfaces for each supplier, and for all processes that involve suppliers, are documented, including any issues.
- Ensure contracts are reviewed as required, with changes to SLAs following under change control.
- Ensure contracts include a change control clause for revisions of the SLAs, managing disputes and an agreed process for termination of the contract.
- Ensure performance is monitored against each supplier's commitments.
- Ensure information is provided for a plan for improving the service.
- Ensure the contract does not prevent the service provider demonstrating control of processes.

Contracts and formal agreements

Supplier management has much in common with SLM, in that it involves agreements on what is to be delivered, but for supplier management this is normally in the form of contracts.

Contracts do not have to be long or complex, but supplier management should recognize the legal status of the formal agreement. For example, disputes and dissatisfaction with the service can have legal implications.

A named individual should be given responsibility for contract management. This gives clarity on roles and responsibilities, particularly when changes are made to the agreed service or terms of service delivery.

Contract precedence will not normally be considered during a Part 1 audit. However, the contract manager and supplier manager (who may be the same individual) need to understand the precedence of the main body of the contract and the schedules. They also need to understand the legal status of any documents that are outside the contract but referred to in the contract. Several documents that exist outside the contract itself, but which may have contractual implications, include service catalogues, service requirements documentation, policies, processes, procedures, glossaries of terms and cost or charging information.

Contractual disputes

Part 1 requires a process for management of contractual disputes between the service provider and suppliers. There should also be agreement on what constitutes a dispute, who will handle the dispute, the way it will be handled and agreed success criteria for dispute resolution.

Service termination

The service termination process should cover the management of risks to both the service provider and customer. For example, protection against loss of key skills as the service approaches termination, ownership of assets involved in delivering the service, confidential information, and the transition of services to a replacement service provider, if this is relevant.

This applies to all types of termination (including transfer to an alternative supplier) but early termination can occur over a much shorter timescale than the expected and planned end of service.

The auditor will not assess the legality of clauses on service termination, but will require evidence that there is a process in place to handle all types of termination, including transfer to another organization.

Trust

Good relationships are based on trust, but trust is not an automatic right in a relationship between suppliers, service providers or customers. Trust is built up over time through each party being honest and respecting the interests and views of the others. Trust, as the basis of a good working relationship, will be undermined if any of the parties involved treats the relationship as a competition, scoring points at the expense of the other.

Risks to a good relationship arise from features such as:

- poor service;
- incompetence, laziness or lack of care;
- using technical jargon at inappropriate times;
- not communicating, 'hiding behind email';
- perceived or actual lack of commitment;
- aggression, dishonesty, evasiveness or visible lack of respect.

The service provider can assess the scale of these risks through satisfaction surveys (collecting both ratings and comments), meetings and the analysis of complaints.

Basic rules for building a good relationship include:

- roles and responsibilities agreed in advance – 'who does what when';
- common interests and goals identified;
- be honest about what can be achieved;
- don't over-commit even if you are under pressure;
- once a commitment is made, meet it on time and to budget;
- accept there should be some give and take – don't be unreasonable;
- remain calm during discussions;
- be positive and constructive even when something is wrong;
- agree meeting times and agendas in advance and stick to what is agreed.

Relationship plan

A good relationship does not happen by accident however well-intentioned the service provider and committed the customer are to making the relationship productive. Building, improving or repairing a relationship should be planned, just like any other aspect of service management, regardless of how intangible the results.

Plans should be developed jointly by the service provider and customer, as well as the service provider and each supplier. If joint plans are not possible because the other parties are unwilling to collaborate with the service provider, the service provider should work on this alone until the relationship has improved and the others parties see the benefit of having a plan.

Key point

A requirement in Part 1, Clause 7.1: '… The [BRM] communication mechanism shall promote understanding of the business environment in which the services operate and requirements for new or changed services.' This could be reflected in a policy on holding business strategy meetings, developing (or contributing to) an IT strategy and managing customer satisfaction using information from surveys and one-to-one meetings with key customers.

Terminology across a service supply chain

It is common that terminology used in one organization does not correspond to terminology used in another. This makes communication between the organizations harder.

A customer might have no interest in the terminology adopted by their service provider and can have a strong dislike of any terminology other than their own. A customer should not be forced to adopt their service provider's terms. Similarly, a supplier and service provider might not use the same terms in the same way, for historic or cultural reasons, even if they have adopted the same best practices.

Standardizing terminology across a long or complex supply chain can be a major undertaking. Differences in terminology should be recognized and managed as they have implications for the design of service reports, discussions in reviews, service catalogues and SLAs.

It is usually productive to map terminology used in each organization. BRM and SLM can provide input into this, as there should be an understanding of the differences in terminology used by the customers and the service provider. For example, the service provider may draw a distinction between an incident, problem, major incident, known error or service request. In contrast, customers can object forcefully if expected to do the same. Supplier management can do likewise for the supplier and service provider.

Other examples of different terminology can include change management, assets, demand management, etc. The aspect that needs most careful consideration is when each party is unknowingly using the same term to mean something different, e.g. 'asset'. Clarity on terminology early in building a relationship can avoid many of the most damaging misunderstandings.

The mapping of terminology used by all three types of organization can become the responsibility of SLM and held in a central repository, such as a catalogue of services, so that the mapping is available and understood by all.

Where terms used by the service provider differ from those in the 20000 series, an auditor will find it useful to be provided with a mapping of the two sets of terms. Although this is not actually a requirement, it will save time and make the audit simpler.

Chapter 10 Service continuity and availability

Introduction

This chapter describes service continuity and availability management.

Major service failures occur for many reasons including denial of service attack, major virus outbreak, access to premises prevented or a natural disaster. Failures can arise from technology, the people who support it and those that use it. The objective of service continuity and availability management is to ensure that commitments to customers can be met in all circumstances. This ranges from localized loss of service through to a widespread disaster.

Requirements have been grouped together in Part 1, Clause 6.3 because the requirements are closely linked and similar. A service provider can choose to implement them as two separate processes or as a single combined process, as long as all requirements are met.

Requirements

The relationship between service continuity and availability management and the customer's service requirements is particularly strong. For example, the following should be understood:

- business priorities for systems and services;
- potential expansion or contraction of business scope;
- changes to locations of customer areas and assets;
- aspects of the service essential to business activities;
- responsibility for decisions after a major loss of service;
- limits to the decision makers' authority.

BRM provides information on the customer's business needs. SLM provides SLAs and a catalogue of services; both are useful sources of information. They normally include availability targets or lists of the most critical systems and services for service continuity planning.

Other processes also provide information. For example, the limits to technology performance, costed options for continuity, information on review results and plans for the PDCA cycle.

The service provider is dependent on the customer for information on business plans, even if a customer does not have a document titled 'business plan'. Examples of this include organizations that, rightly or wrongly, operate on a short-term basis and with little planning.

Even if this is the case, a service provider is not allowed to abdicate their responsibilities for understanding their customer's business and business plan.

Under these circumstances the service provider should develop and document their understanding based on other sources of information. This includes service reviews, market research, customer satisfaction, complaints and sector knowledge. This should then be discussed with the customer to get agreement for it to be used for service continuity and availability management planning. The customers will then be aware that if they have withheld business plans, they have done so at their own risk.

Service providers may have customers that are individual users of an Internet-based service, often referred to as cloud computing. The 20000 series applies to this type of service. However, it is unrealistic for each 'customer' to be approached about their service requirements. Instead, the service provider should demonstrate an understanding of typical service use and requirements, and convert this into effective service continuity and availability plans.

In some cases a service provider does not conform to the service continuity requirements. This failure can be due to inadequate BRM or SLM, and not directly to service continuity and availability management. This particular circumstance highlights that the benefits of service management overall is greater than the sum of individual processes.

It is acceptable if the customer consciously decides to accept minimal service continuity, as long as there is evidence that the customer has understood and accepted the risk.

Assessing risks

An unusually wide range of risks is considered for these processes. This is why the 20000 series emphasizes understanding the service, service components, risks to the service and the way risks can be managed.

The ability to recover services quickly should be balanced against the costs. It may be impossible or not cost-justified for a service to be highly resilient to failure. The customer may prefer to rely on recovering a service in a timely manner at a lower cost.

Key point

Many of the features of the 20000 series are variations on risk assessment and management. For example, '… the service provider shall assess and document the risks to availability and continuity of services'.

This could be directed by a policy on the need for risk management of services, not only as part of service continuity and availability management, but also across other processes, including the PDCA cycle.

Timescales and funding

Availability management analyses, reviews and acts on lost availability, over minutes, days, weeks and months. A long-term aspect is planning for high availability, e.g. building resilience into an infrastructure during its design. Service continuity planning is also long term. Plans can take months to develop. They are reviewed at relatively long intervals, but at least once a year.

Service continuity and availability management plans normally require additional funding for implementation and increases the total cost of the service. This extends the elapsed time for agreement of the plans as top management consider the costs and benefits of investing in the proposals. Without management commitment, availability management and service continuity are usually under-funded and done badly or not at all. Instead the service provider gambles that a major loss of service will not happen.

Developing plans

It is a requirement of Part 1 that plans are developed and then kept current for both service continuity and availability management. The planning approach adopted needs to cater for a wide range of circumstances, including loss of service for reasons outside the direct control of the service provider.

Plans required for service continuity and availability management can be particularly time-consuming to put in place for the first time. This is because the relationships between components such as software, hardware, tools, communications, accommodation, service provider personnel and users are normally very complex and difficult to articulate, so that planning is also difficult. A single item or a link between two

items that is missing from the plans could be the weak link that makes the whole plan fail. Because the relationships between components are complex, planning is also very reliant on effective configuration management. The need for effective service continuity and high levels of availability can trigger recognition of the benefits of configuration management.

The active involvement of a manager with responsibility for the process is most likely to be necessary when requirements are being identified and plans are being made for the first time.

The approach for planning should include:

- customer's business plans;
- service requirements;
- effective changes to requirements affecting the plan;
- service catalogue and SLAs, including:
  - access rights to the services;
  - service response times;
  - end-to-end availability of services;
- procedures to be implemented in the event of a major loss of service, or reference to them;
- availability targets when the plan is invoked;
- recovery requirements;
- approach for the return to normal working conditions.

The availability plan(s) should contain availability requirements/targets. Other useful considerations include:

- service hours;
- critical business periods and maximum acceptable period of lost service;
- maximum acceptable periods of degraded service;
- acceptable degraded levels of service after loss of service;
- dependencies between service and system components;
- role of suppliers;
- a review to check the plans are still appropriate.

Locations

The location selected for storage of data, software, documentation, hardware or office space for use by the service provider's and the customer's own personnel should be physically separate from normal locations and also have separate communication links. Supplier management and configuration management normally play a role in establishing alternative locations.

The service continuity plan(s), any relevant contact lists and the CMDB should be arranged so that they are accessible if the loss of service also prevents access to normal service locations.

Activity levels

The plans should accommodate changes in the size and scale of the workload supported by the service. This includes changes to business activity and workload peaks, troughs and averages.

In extreme cases, not taking changes into account can mean the capacity is inadequate if the service has to be provided from a backup site. Conversely, a decrease in normal workloads can make the plans for a backup site far more expensive than was previously necessary, because excessive capacity has been provided.

There are advantages to planning both service continuity and availability at the same time, as gaps and overlaps are more readily identified and resolved. When multiple plans are used, it is advisable for the separate plans to be closely linked. Typically, this is easiest to do if they form part of a programme and are managed by programme management. This is also an example of integration between components of the SMS.

Return to normal working

Effective service continuity and availability management are dependent on hardware, software, data, documentation, accommodation, facilities and people who are required to return the service to normal. The auditor will expect to see evidence that the requirements and plans cater not only for handling a crisis and the immediate aftermath of a service loss, but also longer term return to service delivery.

Requirements and plans should cover each of the steps for changing the emergency arrangements back to normal services. Depending on the nature of the underlying cause and the scale of the service loss, this could be a major project, taking many months.

The plans should reflect expected changes to business-critical activities over time. For example, end-of-year activities are not important if the service is lost at the start of the new business year. The same loss could even have legal implications in the period immediately before the year end. Emergency arrangements for before and after the end of the year may be very different to those required for the rest of the year.

Typically, return to normal service includes tasks such as retrieval of backup data, software and documentation from storage. This can also involve data problems and reloading of data, as well as consistency issues across systems.

It also typically includes ensuring there is equipment for:

- service restoration;
- service support and delivery;
- users of the service.

It can also be advisable to plan for relocation of the service provider and the customers/users, including consideration of ways for achieving relocation quickly, in case normal locations have become permanently unusable.

Change management

The interface between service continuity and availability management and change management is particularly important because changes can easily have an unintended effect on the ability of service provider to function after a major loss of service. As for other processes, changes to the documents, including plans, produced or used by service continuity and availability management are under the control of change management.

Documentation

Accurate, detailed but easily used plans and supporting documents are an important part of service continuity and availability management. Not only will the plans and documents be easier to understand and use, but they will also be easier to maintain.

At least one copy of all key documents, which are easily identified as the current version, should be stored away from the service provider's normal premises, but should still be easily accessible. Equipment to duplicate, distribute and use documentation is also necessary as normal methods might not work.

Example – After the flood

During severe weather, a distribution depot was flooded when a local river burst its banks. All equipment on the ground floor was damaged beyond repair. Unfortunately, when the service continuity plan was developed, the risk of flooding was not considered. The river was out of sight and out of mind.

The floodwater was so deep personnel were unable to reach the building to execute the continuity plans. After a day's delay, they were able to establish that equipment on the upper floors was still in working order. However, because several components of the infrastructure were located in the basement and ground floor none of the equipment could be connected to head office. For example, power was interrupted and some network hardware was damaged.

After the service was returned to near normal status, a review recommended relocation of vital equipment to the upper floors, with duplicates to be available at short notice from a different location. In the event of a repeat flood, the office could be functioning normally again as soon as staff had access to the building.

The option of having an alternative backup site away from the risk of flooding was considered. This was rejected because a delay in getting access was acceptable if, once the staff were on site, they could resume working quickly.

It was recognized that the original risk assessment had not been done properly and that testing of the plans had not been rigorous enough or frequent enough. The risk of flooding was incorporated into the revised plans but, more significantly, other risks were reconsidered and taken into account in a new version of the continuity plan.

Roles and responsibilities

Immediately after a serious loss of service it is easy for there to be uncertainty about 'who does what and when'. Effort can be duplicated or tasks can be omitted because each person thought someone else was responsible. Planning includes documenting individual responsibilities for 'who does what and when'. This can be done using matrices such as the RACI matrix shown in Chapter 6.

A key individual being on leave or having left the organization without a substitute can become a weakness in the plan. It is usually appropriate to have nominated substitutes for each person with a specific role and responsibility.

One key role in plans is the decision to execute the service continuity and availability plans. That role should have the authority to make the decision, e.g. top management or the process owner for service continuity.

Whoever has this responsibility needs to be given criteria against which a decision can be made. For example, the scale of the service loss, the time it will take to resolve and the impact on the customers at the time the service is lost.

Testing service continuity plans

The service continuity plan is executed only when there is a major service loss, at the very time when a defect in the plan is hard to cope with. It is particularly important for service continuity plans to be tested and re-tested because they are normally complex and subject to frequent changes. The more frequent the changes the more frequent should be the testing.

The frequency should also reflect any legal liability, regulations, delivery of life-protecting services or other high priority service being delivered. Conversely, a service that is stable and used for activities that are not business critical may need testing less frequently, with less rigour and therefore lower cost.

It is advisable for testing to be done with the involvement of the customer, against a set of objectives agreed by the customer and service provider in advance. This is not a Part 1 requirement but benefits the quality of the test and plan.

Effective testing of plans can be time-consuming, expensive and a distraction from day-to-day delivery of the service. However, gaining short-term savings from delaying or cancelling tests is short-sighted. The scale and complexity of effort of improving the plan after it is eventually tested typically outweigh the benefits of avoiding the earlier test costs. The plan can have become so out of date that it has to be abandoned and completely redone. Out-of-date plans also carry risks to the service, which are a hidden cost.

All tests should be done formally, with tests recorded and information on test failures used to develop action plans to correct the plan. Typically, this is input to the continual service improvement plan as part of PDCA.

Happily, the service provider does not have to arrange for a major loss of service to prove they meet the audit requirements. The auditor assesses the development, management and testing of the service continuity plans, not their execution.

Keeping the initiative going

Service continuity plans should be reviewed at least annually. Even the plan for a service that is not business critical should be reviewed to ensure that there have been no major changes in requirements and that the costs of contingency arrangements arising from the plan are still cost-justified.

The reverse is also the case, i.e. a continuity plan could have been developed for a service once of low importance but not changed when the service became business critical. For example, email.

This can be a failure in another process, e.g. BRM failing to pass on information on the customer's business activities to service continuity and availability management. In this case, BRM should also be improved once the failure is identified by the review of the service continuity plan.

It is also advisable to review using test results and after significant changes in:

- the customer's business activity and business needs;
- services;
- the way the service is delivered (e.g. after process re-engineering);
- suppliers and supplier contracts;
- organizational structure of the service provider and customer;
- accommodation (e.g. office moves).

Any change that meets the criteria for a high-risk change, with the potential for a major impact should also trigger a review. These are changes that the change management policy considers need the added protection of the requirements in Part 1, Clause 5, for new and changed services.

Change management should also assess the impact of any change on the availability and service continuity plan. However, it is also advisable to consider the impact on the whole supply chain of services, including suppliers or other groups. This applies to all suppliers, not just those that are specialist suppliers of service continuity or availability services.

Availability and unplanned non-availability should be recorded and compared to targets. Unplanned non-availability should be investigated and appropriate actions taken. These are the only requirements for availability management that are not matched by similar requirements for service continuity.

As lost availability normally has an impact on the customers and users, there is usually an interface to SLM, BRM and many other processes in the SMS.

Chapter 11 Money matters: budgeting and accounting

Introduction

This chapter describes those aspects of budgeting and accounting needed for a service provider to fulfil the requirements of Part 1. This chapter is not limited to the requirements of Part 1, Clause 6.4. It also covers topics useful for a broader understanding of financial management and terminology. This will help, for example, to identify ways to understand the cost of the SMS and services and therefore how to improve cost-effectiveness.

The context

Service providers often provide or rely on shared services, shared resources and a mix of capital and revenue funds. Some service providers charge for their services, others provide sufficient detail to allow costs to be understood for service provision and for service usage by individual departments. Most service providers operate in a complex environment managing financial assets, service assets and information assets. This combines to make budgeting and accounting for services a daunting prospect for those with a service or technical background. For example, service assets and information assets are often not assets at all in accounting terms because they have no resale value.

Why does it matter?

Financial policies, processes, procedures and controls are used to manage financial risk, to ensure control processes are effective, and to minimize fraud.

It is also now recognized that the professional management of a service is only effective if the financial aspects of services are understood. For example, most service providers seek to minimize costs while improving services, either willingly or because they are forced to do so. To do this well, service providers need to understand the way budgets are produced and the way actual costs are tracked against a budget. Service providers

should also have information at a sufficient level of detail to understand costs at service component level. Costs should be understood even when services are not charged for.

The PDCA cycle of improvements relies on the use of financial information for informed decision-making on service improvements, increasing value for money and other changes. Understanding costs means that decisions are based on better information, not just on the nature and quality of the service or based only on technical reasons.

Budgeting and accounting are also part of an overall system of controls that ensure the service provider's organization is operating with financial probity. This should be included when the SMS is planned, operated or improved.

There are parallels between budgeting and accounting and other processes. For example, a budget, which is a set of financial targets, plays the same part in budgeting and accounting as service targets in SLM.

Local knowledge and financial rules

A manager new to working with budgets and accounts should seek guidance from their finance department. Terms differ across countries, even those that nominally speak the same language, e.g. the UK uses the term 'depreciation' and the USA uses 'amortization' for the same thing. Other differences can occur within a single country due to company policies and if alternatives are allowed under national law. This includes rules on the difference between capital and revenue expenditure, what constitutes an asset in accounting terms, rules on depreciation (or amortization) etc.

Advice from the finance department is important for building a budget, developing cost models for services, reporting actual cost against a budget, reviewing financial forecasts and improving cost-effectiveness.

Many service providers will find that financial policies are already established. The financial policies are part of the SMS, even if they are not developed for the SMS, by the service provider. This type of 'ready made' policy avoids the need to develop them for the SMS. They are simply incorporated in the SMS.

Revenue and capital

The rules on the difference between revenue and capital expenditure are important to the operation of an SMS. The rules are influenced by government fiscal policies, accounting regulations and a service provider's own organization-wide policies. There is little flexibility within any one

organization once the policy has been established. For example, once a cost has been classed as revenue expenditure it is not normally reclassified as capital expenditure and vice versa. In some cases deviating from the normal rules is actually illegal.

Revenue expenditure is the accounting term for recurring running costs for an organization. These are sometimes referred to as 'operating costs'. These range from the costs of employing personnel through to small items of stationery. They can be a major expenditure but are not available for resale, e.g. leasing hardware, a subscription service to an online system, telephone line rental. These costs should be fully covered in a single financial year.

Capital expenditure is the accounting term for the cost of an investment in (financial) assets that can be spread (depreciated) over the expected working life of the investment. Capital expenditure, often referred to as capital costs, are mainly one-off fixed costs spread (depreciated) over more than one accounting period. Capital expenditure is recorded as assets that could be sold.

Depreciation is spreading the cost of an investment funded from capital over the working life of the investment. This type of investment is referred to as an (financial) asset. Each year the remaining value of the investment is smaller, i.e. it depreciates in value. Options include 'straight-line depreciation', under which there is an equal reduction in value for each year of the asset's expected useful life. A PC 'depreciated over three years' would be recorded in the accounts as losing a third of its initial value each year.

To be depreciated an asset should:

- wear out, decay, be used up, become obsolete or lose value;
- have an expected useful life of more than one financial year;
- have a life that can be recorded.

Expected working life is set for accounting and budgetary purposes and might not match the actual working life. The cost is spread (depreciated) over the expected working life, e.g. a PC expected to have a working life of 3 years, a server 5 years, office furniture much longer. Expected working life is normally set for each type of investment by some form of financial policy. In some cases the useful working life is influenced by accounting practices, regulatory or statutory requirements. These decisions are often outside the service provider's control, but are acceptable evidence of a policy for the SMS.

After an asset is 'fully depreciated' it can still be in use, with a nominal asset value of zero.

This is a no cost item for the accounts and the investment is fully paid for. Less happily, an asset might have to be replaced before it is fully depreciated. The cost still appears in the accounts and the service provider might also have to pay for a replacement. Alternatively, an accounting adjustment can be made, depending on the organization's financial policies and, in some cases, legislation or regulations on accounting practices.

Depreciation can be a serious issue when seeking support for projects where (financial) assets, such as technology, are to be replaced.

Assets are paid for using capital and are 'things that have been bought', or 'things that have been built'. A common category of asset is fixed assets, which are tangible and can be buildings, PCs, printers or furniture. Assets may be things used in service management or produced by service management. Some service providers also have intellectual property assets, e.g. specialist software developed by the service provider or a trade mark.

Consumables are assets that wear out relatively rapidly or are of such low cost so that depreciation is not worth tracking, i.e. those items that are effectively used in a single financial year.

Categories of costs

Both revenue and capital costs are categorized so they can be identified and shared out across departments, projects, services etc. in an appropriate and predictable way. This is relevant even if the costs are not used for charging. Accounting manages these categories of costs differently.

The cost categories for both revenue and capital are:

1a) fixed or 1b) variable;
2a) direct or 2b) indirect.

1a) Fixed costs: These do not vary with usage or throughput of work. An example is basic salaries for permanent members of personnel. A basic salary is fixed however many hours the person works. Even if someone is on holiday, the basic salary cost is incurred. Another example is the rent for an office.

1b) Variable costs: These are incurred each time a service is used or a product produced. Examples include overtime because in accounting terms it is optional and ad hoc. Other variable costs include stationery and telephone calls (i.e. if you don't use it much, the cost is less, if you use it a lot, the cost is more).

2a) Direct costs: These are measurable, predictable and attributable to a single product, service, customer, cost centre or activity. There is no ambiguity about what creates and influences direct costs and the way the costs are **allocated**.

2b) Indirect costs: These are less easily handled than direct costs. They are overheads shared out (**apportioned**), according to rules defined in advance, e.g. the cost of a service desk used by several customers. The rules for sharing (**apportioning)** costs can create considerable discussion, especially if an apportioned cost is more than expected.

Key point

By effective use of coding for costs and sensible rules for allocation and apportionment of costs, a service provider can identify the cost of service, overall or by department, business activity or location. This can have many benefits, even if the service provider does not charge for services. For example, the cost of a service can be compared before and after a service improvement programme; the cost of different services can be compared or the cost of services during normal office hours, compared to 24x7.

Combining categories

Both fixed and variable costs may be direct or indirect, i.e. fixed costs can be **allocated** as direct costs or **apportioned** as indirect costs. Variable costs may also be allocated as direct costs or apportioned as indirect costs.

For example, the basic salary cost of a support team member is fixed. The fixed cost may be allocated to a single department or apportioned across several departments according to how much time the person spent helping each department. Also, costs such as stationery are variable but may be allocated to one department irrespective of how much stationery is used, or it could be apportioned (shared) across several departments according to what each department has used.

Even if a service provider uses only notional charging or does not charge at all, apportioning and allocating costs helps identify the way costs can be reduced.

Balance sheet

In the way that a CMDB is a data store used to record attributes of CIs, and the relationships between CIs, throughout their lifecycle, a balance sheet is a record of financial status. A balance sheet shows the financial strength and capabilities of the service provider's organization.

Profit and loss accounts are part of the balance sheet. They report on the service provider's profit on sales and the costs of their service.

Identifying and managing variance

In financial terms the difference between a budget and actual figure is a variance. Variances should be investigated and managed before the underlying issues become significant. Using the information in this way should mean that funds are available for the agreed services throughout the year and that the budget is not overspent or spent incorrectly.

Rules are necessary to define acceptable variances and actions to be taken when an unacceptable variance is observed. Actions will depend on the reasons for the variance.

The reasons for variance include:

- changes in the level of customer activity or size of business;
- changes in the number of users or user profiles;
- costs of a response to a major disaster;
- changes in technology;
- the introduction of efficiencies (or inefficiencies) into processes;
- poor identification of actual costs during the budgeting exercise.

One key reason for variance is that most budgets work on the basis that every month is identical. A budget based on 1/12th of the annual figure for each month can be overly simplistic compared to the changes in service delivery costs. Many businesses are seasonal or subject to changes, e.g. telephony costs can show variances due to the service desk changing from being phone-based to remote entry of requests by users.

Variances can be due to unusual events, such as a major virus outbreak mid-year, requiring unusually high levels of overtime. This can mean the service provider is over budget at the end of the year because the unusually high costs cannot be redeemed in later months.

Variances can also indicate that budgeting was done with inadequate information about plans.

Key point

Being under-budget is not necessarily good news as it can be an indicator of lack of control or lack of accurate predictions of what is likely to happen. For example, if the actual basic salary costs are less than the budgeted costs, this could be due to personnel losses. The remaining personnel might be unable to deliver the service levels, compounded by the remaining personnel feeling under pressure and therefore more likely to seek a new role. In this case actions can include management addressing the reasons for excessive turnover, to stem future losses.

If salary costs are higher than budgeted this can be due to an unexpected and unplanned increase in the support workload, requiring more personnel. This needs an investigation into why the workloads have increased, so that action can be taken to return the workloads to their previous levels. If the cause is due to a project creating increased support workload, change management can be used to get the project-related support workload back under control.

Costs might need to be re-forecast if circumstances change. This does not change the actual overall funds budgeted, but makes variances easier to understand and control, month by month, once identified. However, finance departments are usually reluctant to take this step.

Variances can be due to changes in income. Examples include income based on a per-user charge when the number of users changes unexpectedly. Income will change but it might not be possible to change costs in the same timescales.

Variances can be unpredictable, e.g. a merger kept confidential until just before it was agreed. Unpredictable variances can also be caused by a failure to understand the customer's business plans by BRM or to react to it, by SLM. Either circumstance indicates that the PDCA cycle should review the other service management processes, including budgeting and accounting.

Regulatory and statutory obligations

Part 1 requires the service provider to be compliant with the relevant statutory and regulatory requirements. This is to an extent a statement of the obvious. Part 1 cannot affect the need to be compliant to other

requirements. However, it is important to take the statutory and regulatory requirements into consideration when developing an SMS, to avoid an implementation that is later found to be inadequate for meeting these statutory or regulatory requirements.

Audits

An audit against Part 1 is completely separate from a financial audit. The former seeks evidence of the quality and effectiveness of the SMS, whilst the latter is defined by regulatory and legal requirements. The Part 1, Clause 6.4 requirements differ from the requirements to produce a true and fair set of accounts for external purposes, such as filing financial reports under national legislation. However, many of the requirements are linked, overlap or are identical.

Chapter 12 Capacity management

Introduction

This chapter describes capacity management and the role it plays in the 20000 series, in particular the way the requirements in Part 1, Clause 6.5 affect the service provider's SMS.

The objective of capacity management is to ensure that the service provider has, at all times, sufficient capacity to meet the current and future demands of the customer's service requirements and business needs.

Many changes to the SMS can affect capacity requirements and in turn capacity changes can mean capacity is no longer appropriate to the workload and this can affect performance. This is not limited to technical issues, such as storage space or bandwidth. It includes any aspect of the SMS where volumes or numbers can increase or decrease and where a mismatch between available resources and required resources affect the SMS and service.

Scope of capacity management

Some of the greatest risks to capacity and performance arise from the application of capacity management only to technical resources. For example, people are very important resources that should be planned. The 20000 series covers aspects of capacity management neglected when the process is seen as *'something the technical people do*'.

The whole of service management, the service and the customer's business activities will suffer if capacity management is restricted to technical resources. Bad decisions will be made, based on inadequate information. In contrast, correctly applied capacity management will interface directly or indirectly with all processes in the SMS, including the PDCA cycle for improvements as well as the service management processes.

Characteristics

Capacity management is fundamentally proactive, with planning and predictions core to the requirements of Part 1. This is also why the process is so closely linked to current and projected service requirements, which are in turn based on an understanding of the customer's business needs. This can span several customers and services. It can be relatively complex under a shared service model where different groups operate completely independently of each other. Aspects of capacity management are closely linked to resource management in Part 1, Clause 4.4.

Agreeing requirements

Under Part 1, Clause 6.5 a service provider is required to identify and agree capacity and performance requirements with customers and interested parties. To do this many other processes play a part and many people can be involved. An example of capacity information flowing between organizational groups is given in Figure 9 below.

Capacity management has strong links to SLM and BRM. Capacity and performance requirements may actually be agreed with the customer via these processes, with no direct contact between those responsible for capacity management and the customer.

A customer should not be required to understand a highly technical specification for their capacity and performance requirements. Instead, the customer should be asked to help develop and then agree a document that defines the end result of the process in terms appropriate to their business activities, e.g. response times and service hours.

Key point

> Many aspects of capacity management and performance can be tied to peak hours of activity, on the basis that if the performance is acceptable at peak periods, it will be even better at periods of low activity.

Interested parties involved can be several different groups, as described in Chapter 2. For example, a supplier needs to know what they are required to do to contribute to the overall capacity and performance management. Other groups could be those involved in agreement of

budgets, service and business continuity, as well as managers responsible for ensuring the service provider meets regulatory and statutory obligations.

Planning

The capacity management plan is an important requirement. Many service providers have a capacity planning or management team that focuses on planning for technical issues such as infrastructure. A specialist team of this type is not often involved in predicting, planning or managing the capacity of other resources. For example, the number of people required by a service desk or the resources associated with the performance of an application.

In practice, many service providers allocate responsibility for managing capacity of different types to different teams. A service provider may do this without actually allocating the name 'Capacity Management' to any of the teams. This aspect of capacity planning can be allocated to managers responsible for a process or to operational managers. For example, a specialist support group will plan for the number of support staff and the hours they will need to work after a new system is made operational. Some of this planning may be done as part of projects, such as the design of new or changed services.

There are many advantages if the skills used for technical capacity management are also being applied to non-technical capacity, e.g. workload modelling and prediction of future capacity and performance.

Peer group review of workload and performance projections and capacity plans can also improve the quality and reduce risks to the service. Typically, this also means that information will flow between many different organizational groups.

Part 1 includes a number of topics for the plan:

- current and forecast demand for services;
- expected impact of requirements for availability, service continuity and service levels;
- timescales, thresholds and costs for upgrades to service capacity;
- potential impact of changes due to statutory or regulatory requirements;
- potential impact of changes to contractual obligations;
- changes from any planned reorganizations in any of the groups involved in delivering service;
- potential impact of new technologies and new techniques;
- procedures to enable predictive analysis, or reference to them.

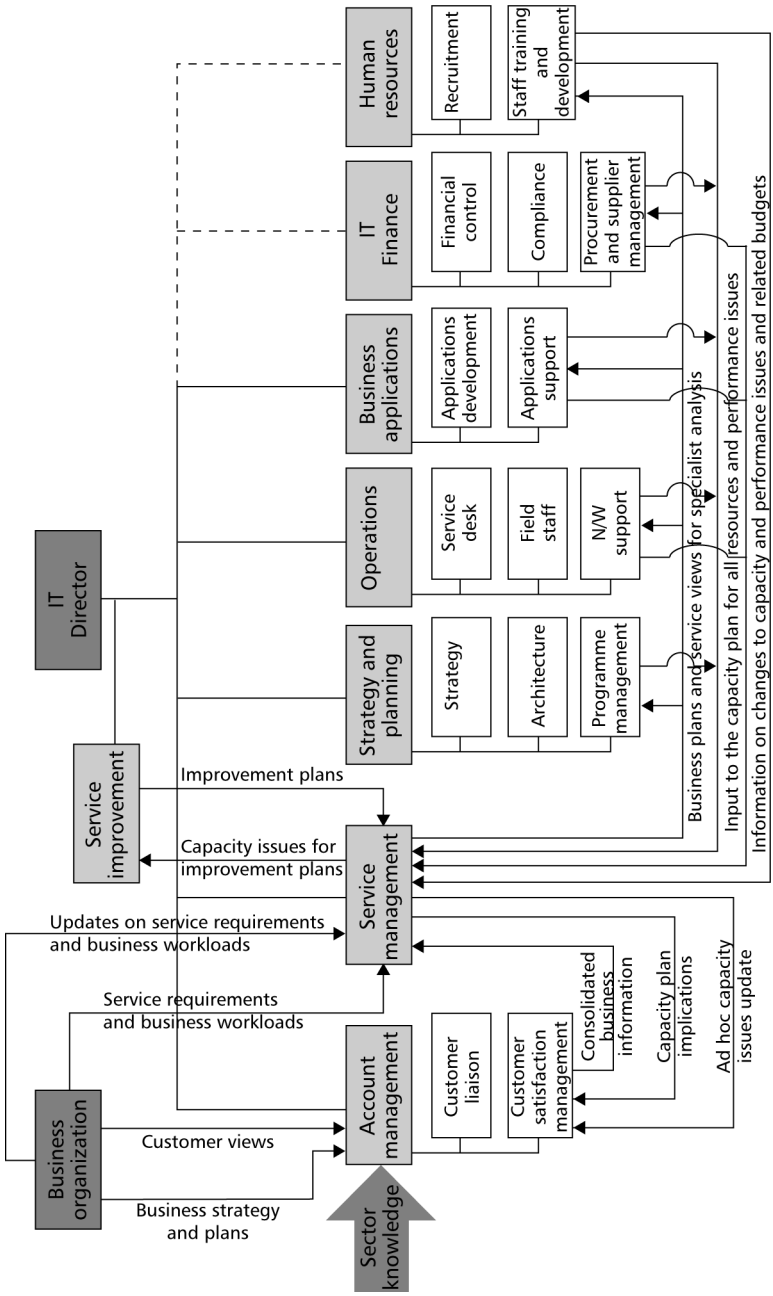


Figure 9 – Example data flow between organizational groups

Providing the capacity

A high proportion of the cost of delivering a service is due to providing capacity. If this is based on 'just in time' purchase of resources there are risks to the SMS due to unexpected delays in obtaining additional resources. There is also limited opportunity to negotiate on the price. Better planning and prediction also allow existing resources to be used more effectively, avoiding the need for new resources. Like all proactive aspects of service management this is linked to the identification of improvements from the application of the PDCA cycle.

Most aspects of capacity management involve financial understanding and decisions. At the most basic level, funds have to be available to pay for the capacity required. This includes both capital used for purchase of (financial) assets and revenue for the day-to-day operational running of the capacity. This in turn has to be managed in a way that meets the requirements of Part 1, Clause 6.4, for budgeting and accounting, as described in Chapter 11.

If the capacity planning, budgeting and accounting for services have been done correctly, the funds should be available, when required, to procure new resources. However well capacity planning is done, this is not always an easy stage and funds are sometimes diverted to another initiative. Aspirations and enthusiasm for increased resources and the performance improvements they bring are often reduced when the cost implications are finally understood.

After such an occurrence capacity management often has to return and do 'what if?' type modelling. What is the minimum acceptable performance and how much will that cost? What can be done with the funds available? After implementation of the new resources, can a more acceptable way of allocating and apportioning the costs be identified? Options for making the best balance of funds invested and the performance to be gained will be required.

Updating the capacity plan

Whatever the final decision, the additional resources are then provided as agreed and the capacity plan is updated. The accounts should be updated and also the budgets planned for the following year could need to be adjusted. Plan updates need to cover all aspects of the resources affected: personnel, technical, information and facilities, etc. For example, increasing the number of PCs when a new customer location is set up also means more personnel are required for support. These people in turn will need accommodation and facilities.

Controlling the changes

The capacity plan may physically be a series of connected plans covering many different initiatives and types of resource.

Changing the capacity of one type of resource can be seen as a localized issue of no interest except to those who use that resource or those who support it. However, by its nature, a resource rarely acts in isolation. Changing one resource usually impacts another. The risk of failure is reduced by applying change management. Part 1, Clause 6.4 requires all such changes to be controlled by change management as a direct consequence of the need to understand and reduce risks.

Example – Why following the process is important

A service provider encountered difficulties because an old server had too little space, preventing access and use. The server was upgraded with additional memory and initially this was seen as a success. However, it was realized after the server failed that the backup had not worked after the upgrade. The customer's business-critical data was lost as a consequence.

The person responsible for the change had not put the upgrade through the change management process because 'it was such a simple change'.

If the correct process had been followed this would have been avoided because it would have been clear that there was a limitation from the CMDB.

Chapter 13 Information security

What is information security?

The objective of Part 1, Clause 6.6 is to preserve confidentiality, integrity and accessibility of information assets. This chapter describes information security as part of service management.

Due to the rapid growth in use of technology, combined with increasingly common attempts at electronic fraud there is now greater risk of information security incidents. Part 1, Clause 6.6 is a set of requirements which, if implemented correctly, will reduce these risks. Part 1, Clause 6.6 also refers to the 27000 series of standards. These cover information security and those interested in service management will also find the 27000 series helpful.

Policies and objectives

Information security is the result of policies, objectives, controls, processes and procedures that together minimize risks to information assets used by or produced by an SMS.

The policy and objectives also take into consideration statutory and regulatory requirements. Contractual obligations on information security should also be taken into account where they are applicable.

As with other policies and objectives required by Part 1, the information security policy should be approved by the service provider's management.

A breach of a security policy can have serious implications, including legal action and even imprisonment. 'I didn't know' is not an acceptable excuse.

Examples include security policies relating to:

- protection of personal data;
- abuse of email or using the Internet for purposes that are forbidden;
- the audit trail of how financial decisions were made.

It is therefore particularly important that the information security policy is communicated to all those involved, including suppliers, the service

provider's managers and personnel, customers and users. If necessary, communication should be supported by training.

Controls, described below, are essential to fulfilling the policy, meeting objectives and managing risks.

Risks

Part 1, Clause 6.6 requires the service provider to define the way they will manage and mitigate information security risks. This involves the linking of policies and objectives to processes and procedures. As some risks are inevitable, the management of information security risks takes into consideration the nature of each risk, the way they will be defined and if possible quantified. Decisions should be made on what risks are acceptable risks. The service provider should develop criteria for unambiguous identification of risks, based on parameters such as likelihood or potential impact of the risk and the implications for compliance with regulatory or statutory obligations.

It is particularly important for successful management of risks that levels of authority, responsibilities and roles are understood for information security. This understanding spans not only the service provider's personnel, but also the various other groups involved, including customers and suppliers.

Risk assessments and security audits

Reviews, internal audits and other assessments are activities included in many clauses in the 20000 series. Information security is no exception. Part 1, Clause 6.6 includes requirements for risk assessments and information security audits. Risk assessments are also relevant to other parts of the SMS, for example, the design and introduction of new services, many aspects of service management and the continual improvements from the PDCA cycle.

The frequency and nature of risk assessments and security audits should reflect the security policy and objectives as well as the type of risk being assessed. The auditor will expect to see that risk assessments are done at a frequency appropriate to the nature of the risk, the nature of the information asset and the implications for the customer's business activities.

The risks assessed or audited should cover compliance with the controls, risks to the controls and risks to the rest of the SMS.

Weaknesses identified in controls should be reported. Some of the weaknesses can be sensitive for protection of information. If this is the

case, the report needs to be restricted to people with suitable security clearance. A weakness, if widely known about, could be exploited, e.g. a reported weakness in the policy on passwords can make it easy to gain illicit access to credit card details. When a weakness is identified a control should be changed, added or removed to reduce the risk. This may be directly controlled by the PDCA cycle of improvements, or controlled centrally but implemented locally, depending on the nature of the change. The changes to controls should be subject to change management, regardless of the way they are actually implemented.

Not all risks are equally serious, e.g. a risk can be life-threatening, so action should be taken quickly. In contrast, if a security breach is only an inconvenience, action can be low priority.

Audit results should be reviewed to identify opportunities for improvement.

Information security controls

ISO/IEC 27001 is a based on a set of controls and control objectives. As a consequence Part 1, Clause 6.6 also refers to the implementation of controls and control objectives. Those mentioned in Part 1 are physical, administrative and technical security controls. The 20000 series does not include details of which controls are to be used within these categories. However, some controls from ISO/IEC 27001, Annex A, that are relevant to the 20000 series are included as illustrations, in Table 14.

The controls in Annex A of ISO/IEC 27001 use the verb ‘shall’. This verb is used for the requirements in International Standards, including Part 1. Annex A of ISO/IEC 27001 describes the risks that each control is used to prevent. The way the controls are operated and how they will be maintained and improved is also included. The service provider should make it clear how the SMS supports the information security controls required by customers and suppliers.

Controls may need to change over time, e.g. if there is a change to the customer’s business activities, service requirements, geographical locations or supply chain arrangements etc. Changes will often be cascaded down via changes to policies and objectives.

Table 14 – Controls and objectives from ISO/IEC 27001

Objective: To achieve and maintain appropriate protection of organizational assets.	
Inventory of assets	Control: All assets **shall** be clearly identified and an inventory of all important assets drawn up and maintained.
Objective: To ensure that information receives an appropriate level of protection.	
Information classification guidelines	Control: Information **shall** be classified in terms of its value, legal requirements, sensitivity and criticality to the organization.
Objective: To maintain the integrity and availability of information and information processing facilities.	
Information backup	Control: Backup copies of information and software **shall** be taken and tested regularly in accordance with the agreed backup policy.
Objective: To prevent unauthorized user access, and compromise or theft of information and information processing facilities.	
Password use	Control: Users **shall** be required to follow good security practices in the selection and use of passwords.
Objective: To prevent unauthorized access to networked services.	
Policy on use of network services	Control: Users **shall** only be provided with access to the services that they have been specifically authorized to use.
Objective: To ensure that security is an integral part of information systems.	
Security requirements, analysis and specification	Control: Statements of business requirements for new information systems, or enhancements to existing information systems **shall** specify the requirements for security controls.
Objective: To avoid breaches of any law, statutory, regulatory or contractual obligations, and of any security requirements.	
Identification of applicable legislation	Control: All relevant statutory, regulatory and contractual requirements and the organization's approach to meet these requirements **shall** be explicitly defined, documented, and kept up to date for each information system and the organization.

Access rights

The Part 1, Clause 6.6 requirements include managing risks from access to information or services by external organizations. This includes a requirement to identify external organizations that need access to information or services. Once they have been identified, controls should be developed, agreed and implemented for management of the risks from access by external organizations. External organizations are normally the 'other parties' managed under Part 1, Clause 4.2, governance of processes operated by other parties.

Suitable controls and requirements for information security include:

- demonstrating accountability for the processes and authority to require adherence to the processes;
- controlling the definition of the processes, and interfaces to other processes, in Clauses 5 to 9;
- determining process performance and compliance with process requirements;
- controlling the planning and prioritizing of process improvements.

Changes

Information security breaches are normally a minority of the events managed by a service provider. Risks can be minimized by careful attention to information security implications during change management. It is also equally necessary to consider the potential impact on the information security policy and controls of other changes. These can range from a simple change to an incident record through to a change to the overall service management policy.

When something goes wrong

The word 'incident' is used with a broad meaning in the 27000 series, to indicate that 'something is wrong with the service'. The 20000 series draws a distinction between incident, problem, known error and major incident, for different aspects of 'something is wrong with the service'.

Under the requirements of Part 1, Clause 6.6 a security incident is managed by incident management procedures in Part 1, Clause 8.1. However, once recorded by incident management the service provider's personnel could then realize the information security incident is actually a problem, major incident or known error. This decision should be based on review of the incident management record.

The information security incident could require a different process or procedure to be applied and other aspects of resolution to take effect, as

described in Chapter 14. It can also be possible that service continuity and availability management in Chapter 10 will be required for the next stage of managing the security incident. For example, a single user can report a virus that is a known virus, with a known resolution and which is a low risk to security and services. For information security this would be a lower priority than an information security breach of the payment service in a customer's main website to steal credit card details.

Because of the interfaces between the processes, Part 1, Clause 6.6 imposes specialist requirement on Clause 7 resolution processes. The priority allocated to the incident should be appropriate for the scale of risk resulting from an incident affecting information security. Similarly, the person or group the incident is referred to can also be affected. This is particularly the case if the security incident record includes data that should be kept confidential, such as a use profile, details of a criminal act etc.

The resolution processes are also required for support of analysis of the types, volumes and impacts of information security incidents. The results are reported so that they can be used to identify improvements to any aspect of the SMS and service.

Chapter 14 Resolution processes

Introduction

The resolution processes are incident and service request management and problem management. The resolution processes all have the objective of allowing the user to continue with their normal activities as quickly as possible. The resolution processes are often the first to be implemented by a service provider. Incident management has a relatively fast pay-back period and it is usually easy to persuade people that it is sensible.

To a user, an incident can be indistinguishable from a service request or a problem. For many users, each of the three is simply something that prevents them carrying out their normal duties. The 20000 series draws a distinction between the processes because each is managed differently.

Incidents and service requests

An incident is usually an interruption to a service but can be a low quality service or the threat of a service interruption. A service request is either a simple request for information or a simple change such as access to a service. Although incident and service request management follow two separate procedures the same stages are usually suitable for both:

- recording;
- allocation of priority;
- classification;
- updating records;
- escalation;
- resolution;
- closure.

Other recommended actions include consideration of security issues and first-line customer liaison.

Many incidents are events that are an annoyance to the user, but are resolved within minutes because they do not require investigation. Incident records are closed when normal service is restored, even if the underlying cause is not resolved or even understood. Seeking the

underlying cause is in the scope of problem management. One type of problem referred to as 'known error' is described in more detail below.

Major incidents

It is important to recognize that although a high proportion of incidents can be easily resolved, incidents can vary widely and some can have a serious impact on the service and on the customer's and user's business activities.

Major incidents can take hours or even days to resolve. They have much greater impact than normal incidents, require additional resources and can be complex to resolve. The term major incident is used, although many major incidents have an unknown cause. Many major incidents more closely resemble a major problem as they require the same type of investigation of root cause.

The service provider establishes agreed guidelines or rules for identifying and classifying a major incident. This should be agreed in advance and understood by all involved, so that they are not managed on an ad hoc and variable basis. The service provider should only declare a major incident if there is a crisis, because major incidents involve deviations from normal resolution procedures. The service provider should be sure that the risk of deviation from normal practices is really necessary.

'Major incident manager' is a role included in the 20000 series. It is advisable for this role to be given to someone with the authority to control all activities, some of which will be unpredictable. This includes the authority to invoke escalation procedures, communicating directly with the customer and with top management. It is not managed in the same way as a normal incident.

It is regrettably common for the major incident manager to be undermined by misguided colleagues. This can be because they are under personal stress because of the scale of the major incident. Whatever the cause, it is still bad practice. Top management should prevent this happening by making the authority levels of the major incident manager clear to everyone. For example, they themselves should defer to the major incident manager on communications with the customer and other top management.

The authority of the major incident manager is likely to be undermined if the person allocated to it has less authority in their normal role or lacks sufficient assertiveness, even if they have the most appropriate levels of technical skill.

Repeated problems with authority being undermined can indicate that the selection criteria for the major incident manager are unsuitable, not understood or being ignored. Whatever the cause this should be corrected.

Major incident co-ordination and review

The identification of a major incident triggers a process that caters for the scale of work (and the number of people) involved in and affected by the incident. Major incidents typically involve several people, often in different teams and locations, working in parallel. They are usually co-ordinated by the major incident manager.

Communication and co-ordination can be difficult but is exceptionally important. A major incident that lasts for more than a few hours also requires the handover of responsibility from one individual to another. The changeover has to be communicated to the service provider's managers, personnel and to the customer. This is also similar to handover of a problem.

It is important for a review of the way the major incident was managed to be completed. This will normally identify correction, corrective actions and opportunities for improvements input to the PDCA cycle for risk reduction.

Problems

Problems typically take longer to resolve than incidents. Problems are defined by Part 1 as the root cause of one or more incidents, where the root cause is not usually known at the time a problem record is created. Problem management has the objective of minimizing disruption to the service by identifying the cause and managing problems to closure.

Problem management also prevents the recurrence or replication of incidents. This includes identifying, planning for and implementing correction, corrective actions or improvements identified by investigation into root causes.

Root cause analysis benefits from the application of structured techniques such as Kepner Tregoe, brainstorming, Ishikawa.

Problem management has many similarities to availability management, described in Chapter 10. Both analyse, review and take action over similar timescales.

One of the objectives of problem management is to reduce the workload handled by incident and service request management. This makes the

service more reliable, cost-efficient and effective. In turn problem management will be seriously limited without information from incident and service request management.

Minimizing the impact of problems

It is necessary to have enough information to understand the actual or potential impact of a problem on the customer and then minimize or avoid that impact.

The problem management procedure should define the data required to identify the scale and nature of the impact, not only in technical terms but also in the customer's and user's business terms. This can extend to the classification method for referencing existing problems and changes, so that the relevant data on incidents, problems and changes are linked. This adds value to the information derived from the separate records as well as reducing risks.

Access to configuration management data is important and can play an important role. Additionally, anecdotal evidence should be collected from customers, users, colleagues and monitoring systems.

The procedure should cover the use of this information to identify options for minimizing the impact of the problem and any associated incidents, e.g. a manual alternative, removal of a defective feature or temporary use of alternative hardware and software. Minimizing the impact also includes communicating effectively with the customers and users, so that they understand how long the service is likely to be affected and what alternatives they have.

Handover of responsibility

Because many problems continue over several hours or days it is advisable for a procedure to include the ways the following will be managed:

- changes to the identities of those responsible for problem resolution during the lifecycle of each problem;
- when and what information is provided (and to whom);
- any escalation required and what should trigger the escalation;
- breaches of service level targets;
- resources used in management of the problem;
- actions taken.

Tracking and updating records is particularly important when several groups are involved in investigation and resolution at the same time. More commonly, several groups are involved because the problem record is reassigned from one group to another during investigation.

The information is also required for subsequent review of the process and the way the problem was managed and resolved, for input to a database of known errors or for development of a workaround.

Known errors

A known error is defined in Part 1 as a problem that has either an identified root cause or method of reducing or eliminating its impact on the services by working around it, or both.

Part 1, Clause 8.2 includes a requirement that problem management is responsible for ensuring that information on known errors and corrected problems is provided and kept up to date. The personnel responsible for problem management are usually responsible for ensuring that other personnel resolving problems provide the correct information. This can involve checks on the quality of data logged on individual problems and the quality of the known error details.

It is important that all known errors are recorded against the service that has been affected or could be affected, as well as the identification of the CI thought to be at fault. Being able to link the known error to a service or number of services will help predict the impact if there is a recurrence.

The information is also useful for the setting of priorities and targets, for scheduling of resolution, for communications with customers and users and for identification of a permanent fix. Similarly, being able to link the known error to a particular CI, or type of CI, has the same uses. This requires access to the relevant configuration management data. Potentially it also requires access to other records, such as those of change management and SLM.

Some known errors are introduced into the live environment as part of a release of hardware or software. This is most likely when the benefits of the new release outweigh the costs of the error. This should be documented as a known error and covered by training, with any known workarounds being included.

Known errors are also closed by problem management when a permanent fix is finally applied or the affected component or service is removed. Known errors details should not be removed until it is established that the permanent fix has been successful. This is commonly done as part of change management.

Known errors may be left unresolved indefinitely. This is because resolution (or even a workaround) can be too expensive or not carry enough benefit to the business. In order to minimize the impact of problems the advantages and disadvantages of leaving the known error

or applying a permanent fix should be documented and considered, including the costs and risks. The decision-making can involve the customer via SLM or BRM.

Workarounds

If a permanent fix is not to be applied or is not yet available, it is advisable to find a method of working round it. This might have no effect on the underlying cause but allow the service to be used. Typical examples include when a permanent fix is not technically possible, cannot be applied in the short term or where a permanent fix is not cost-effective. For example, the benefits of upgrading to the next version of an off-the-shelf package to avoid recurring incidents may be outweighed by the need for expensive architectural changes.

The decision on whether to replace a workaround with a permanent fix can involve many of the other service management processes. For example, the decision may involve the customers, usually via SLM and/or BRM. Also the financial processes can contribute information for a decision on cost-effectiveness of a permanent fix versus a workaround being left in place.

Part 1 does not specify when a workaround should be replaced by a permanent resolution of the underlying incident. However this is done it should be done effectively and documented.

Information on workarounds is usually held in a knowledge base suitable for control of the information. The service provider could hold information such as:

- the circumstances under which the workaround is used;
- components of the service the workaround applies to;
- underlying cause;
- symptoms of the incident avoided by applying the workaround;
- business area affected;
- the scale and nature of the impact;
- effect of the workaround;
- residual impact after the application of the workaround.

There are no requirements for the nature, format or contents of a knowledge base used for this purpose, or the methods used to access the information it contains.

Preventive action

Effective problem management leads to a reduction in repeat incidents and problems, not just the effective handling of those that do occur.

Information used for analysis of causes, identification of options for a permanent fix and problem avoidance includes:

- gap between service levels and targets widening;
- trends, e.g. recurring problems and incidents, known errors;
- recurring problems of a particular type, component or location;
- configuration management (including asset management);
- change management;
- known errors and workarounds (including from suppliers);
- historical information on similar problems.

Problem prevention may cover a single incident or a series of related incidents, a major incident or problems. Examples include repeated difficulties with a particular feature of the system, such as a tendency for a PC to 'hang' requiring rebooting. At the other extreme, there are changes that require major investment, e.g. the replacement of an unreliable infrastructure.

Proactive problem management identifies weaknesses, such as a single point of failure (high risk and possibly high impact). Having identified the weakness and risk, options are proposed for preventing the risk becoming reality.

Advice and guidance

Problem management provides information on the ways to avoid a defective feature or how to use the feature correctly. This information is often referred to as frequently asked questions (FAQs) and can extend to training being given.

Problem reviews

The effectiveness of problem resolution should also be monitored, reviewed and reported. Problem reviews of unresolved, unusual or high-impact problems are likely to help the reviewer identify process improvements, as they test the resolution processes under extreme conditions so that any weakness is more likely to be identified.

Changes to the resolution processes could also be required as a result of a change to the nature of the service or support workload. Review and improvements in the process are particularly advisable when the process is newly implemented.

Any opportunities for improvements identified should be input to the check stage of the PDCA cycle, specified in Part 1, Clause 4. This minimizes the risk that a single process will identify improvements that are not compatible with other improvements or changes.

If other processes are changed it is usually necessary to realign resolution management with the changed processes and vice versa. Similarly, changes to targets in SLAs can mean changes to problem management. Changes to the complaint procedure in BRM can mean that escalation managed by problem management might have to be changed.

If incident or problem resolution involves a supplier, a link to supplier management can be needed for problem reviews. The scope of the problem review is far from only technical issues.

It is recommended that other deficiencies are reviewed, including:

- deficiencies caused by resourcing, training or documentation;
- personnel commitment in resolving incidents and problems;
- nonconformities, e.g. against standards, policies and legislation.

The seniority of those involved in the review should be based on the impact and risks. The manager(s) that owns the resolution processes and top management might need to be involved. This is particularly the case if personnel feel that their credibility has been undermined and that they will be blamed for a service loss.

Common features of resolution processes

The importance of records

Incidents, service requests and problems can be reported by telephone, during visits, by voicemails, letters, logged directly by users or by monitoring tools that record when certain fault types are detected. All should be recorded.

Some service providers record only events that are not resolved quickly, under the impression that if an incident is resolved quickly it does not matter if it is not recorded. Part 1 does not explicitly require all incidents, service requests and problems to be recorded. However, if this is not done the service provider will find it difficult to fulfil other requirements, such as providing information on incidents to problem management, problem management analysing trends or the development of known error details.

The resolution processes also provide information to several other processes, e.g. records, usually in aggregated form, flow to service reporting, or if a change or release has failed information is provided for process improvement planning.

Details of the cause of the failure should be added to the record. For an incident, this is known at the time the record is raised. For a problem, the record should include the way the resolution was handled and details of the resolution.

There is no explicit requirement in Part 1 to inform a user who reported an incident or problem or made a service request, when the record is closed. However, it is advisable that a record is closed only when the user is given the opportunity to confirm that it has been resolved. When many people are impacted it is usual for service providers to contact selected individuals or to use a senior-level customer as a contact point.

Depending on the nature of the incident or problem and the way resolution was achieved, it can be appropriate during record closure to ensure that the user is aware of the way the problem was resolved.

It is also recommended that if resolution is not possible the customer is informed of the circumstances if the record is to be closed. This is appropriate irrespective of whether a workaround is possible.

A record should be checked before closure to ensure that all the required information is present and correct, e.g. incidents and problems are classified correctly.

Priorities

Priority is used throughout service management to manage workloads effectively but is pivotal for the resolution processes. Priority needs to take into account the customer's and users' priorities, so these have to be understood. For example, what impact is there on the customer's business? An incident can seem trivial to the service provider, but could have a huge impact on the customer's business activities.

In practice it is also advisable to understand potential impact. If nothing is done immediately because the business is not impacted at that time, when will it start to matter to the customers? If a fault occurs out of service hours when there is no one relying on the service, how long will it be before the service is needed? Similarly, a failure in the end-of-month processing has low impact at the start of the month, but will become high impact at the end of the month.

Scheduling based only on priority can result in conflicts over which high priority problem should be allocated scarce resources, or the cost–benefit of working out-of-hours to provide a faster resolution.

Priority-based scheduling for resolution processes should therefore include:

- priority;
- skills available;
- competing requirements for resources;
- effort/cost to provide the method of resolution;
- elapsed time to provide a method of resolution.

By scheduling and setting a target time, it becomes easier to develop procedures for communications between the groups involved and between the service provider and the customer or user. If service targets cannot be met, the service provider should inform the customer and interested parties and escalate if necessary.

Key point

Many service providers rely on guidelines for assessment and allocation of targets based on priority, to provide a consistent approach. In practice it is advisable to link the agreed priority to a timetable for action, so that high priority is acted on very quickly; low priority is scheduled to be handled whenever the resources become available.

The most common timetable is to link each category of priority to the maximum time within which the event will be resolved and to provide an indication of how many are expected to be in each category. It is advisable to check that classification is being done consistently. Classification can become inconsistent over time as new people get involved, perhaps without enough training.

Managing and minimizing impact

Part 1 requires that resolution processes include management of the potential or actual impact of service failures. This has to be done with an understanding of the customer's business and the business area, users or activity affected. This information is required so that decisions on minimizing the impact can be taken on an informed basis, as described in the following section. This type of information is also used in establishing priority, to set a target for resolution and for workload scheduling.

Information on the impact is useful for problem management, e.g. individually, trivial incidents recurring frequently can have an overall major impact that needs attention so that recurrence is prevented.

In order to meet the requirements for managing impact it is advisable for procedures to define how to get help from technical specialists. Many organizations develop a knowledge base of skills and contact details, with suitably-skilled people available during the hours when help can be needed. Similarly, access to documents such as processes, procedures and work instructions.

Information on similar incidents can quickly provide insight into the reason an incident occurred and ways it can be resolved. In some cases the information on an incident can be linked to a problem management investigation. If none of the information on previous incidents matches the new incident, recognition that this is a new incident will provide useful information for resolution should the incident recur.

A degraded service provided quickly can be preferable to a normal service delivered much later and each case has to be judged on its merits.

Keeping the customer informed

The customer should be kept informed on progress. Even an apparently trivial event can be a source of annoyance to a user, particularly if the user is left without information on what will happen and when it will happen.

It is important for information on the likely time for resolution to be provided, so that the user can plan around the expected timetable. It is equally important that the customer is alerted if their expectations will not be met, e.g. a service target will not be achieved. This is in case escalation is advisable.

A decision on 'who should be told what' is best agreed in advance, so that it can be done quickly and reliably when required. Some service providers use online bulletin boards or provide access to the incident logging system, so that customers and users can check on the progress of an incident or problem.

Escalation

If the normal processes and procedures for resolution are not enough, escalation will be necessary. Escalation may be triggered by one or more of:

- recognition that additional knowledge is needed for resolution;
- resolution has not or will not meet the agreed target time for resolution;
- resolution has been badly dealt with or given too low a priority;
- too few resources are available or allocated.

Escalation may involve referral to more senior management in order to agree the provision of more resources and possibly expenditure. Escalation may also involve referral and involvement of people of the same seniority, typically if different skills or more resources are required.

Escalation procedures work far more effectively if they are agreed in advance. It is advisable for the escalation procedure to include the conditions that will trigger escalation. For example, size of problem, time for resolution, and scale of actual or potential impact on the customer's business activities. It is also advisable to include what happens during escalation, and who becomes involved at what time.

Chapter 15 Configuration management

Introduction

This chapter describes the key features of configuration management required to establish and maintain the integrity of identified services, service components and configuration information.

The requirements for configuration management in Part 1 cover:

- identification: selecting and defining CIs;
- control: ensuring that only authorized CIs are used and maintaining the integrity of systems and services;
- recording: changes in CIs and their status in the CMDB;
- reporting: providing access to configuration information, with different views;
- auditing: CIs and the CMDB records for nonconformities.

What is effective configuration management?

The process should be based on the service provider's and customer's business drivers and supporting policies and meet the requirements of the rest of the SMS. The degree of control should be planned and take into consideration the service requirements and risks associated with the configurations and CIs. For example, business-critical services can require a greater degree of control compared with other services.

An effective process provides the configuration information to plan, maintain and track all changes to CIs. The process provides different views of the current and planned state of the services and service components for different roles.

This helps those involved to:

- relate technical components to services and to business needs;
- understand the risk and impact of changes;
- understand the relationship between planned changes;
- identify the root cause of incidents and problems;
- find configuration information quickly.

Table 15 allows configuration management requirements to be traced back to the original business requirement. This is particularly useful when a change fails or a problem is being investigated. It also helps the identification of nonconformities, such as:

- CIs that do not meet requirements;
- unauthorized CIs, e.g. user-introduced software;
- components that need to be replaced;
- CIs that have been changed without authorization.

It is recommended that automation is used to improve efficiency and effectiveness.

Table 15 – Mapping back to the business requirement

Business requirement	Configuration management requirement
Adherence to legal regulations for the use of software assets	All software assets and related assets are identified and managed in countries where the legal regulations apply
Regulatory control of business processes that are fundamental to the financials of the company	Financial assets are identified and managed. Components that support the security and integrity of data for financial processes will be uniquely identified and will be traceable back to their original requirement
Reduction in the operational risks to critical services	Changes with the potential to have a major impact on services or the customer are defined according to defined criteria. CIs can be classified by risk. High-risk items include: • critical services; • new technology within the organization; • items that cause major incidents; • items that cause outages; • single points of failure; • internal and external interfaces; • security perimeter

Scope of configuration management and CIs

The scope of configuration management is defined by the scope of the SMS. The minimum effective scope should be documented, including:

- services defined in the service catalogue;
- CIs required to deliver the services, e.g. desktops;
- software and licences, e.g. applications;

- CIs in the underlying infrastructure that require maintenance, e.g. upgrades.

In Part 1, Clause 4.1.4 the management representative's authorities and responsibilities include ensuring that assets used to deliver services are managed according to statutory and regulatory requirements and contractual obligations.

Key point

The scope and level of detail for configuration information are both important for an effective process. If the scope is too wide because too much detail is held about CIs, effort will be wasted in maintaining information that is of no practical use. If there is too little detail there will be a lack of control and lack of visibility required for effective use of the information by other service management processes.

Interfaces

The control processes should be integrated with the rest of the SMS and those of its customers and suppliers. To achieve this requirements are agreed with the customer via BRM and with suppliers via the supplier management process. SLM would normally be involved as this links suppliers, the service provider and customers.

It is the service provider's responsibility to define any requirements placed on suppliers. The service provider should retain overall governance of any processes operated by other parties, such as suppliers. This applies even if the service provider's processes are tailored to accommodate a supplier's environment.

It is recommended that there is a planned approach to managing suppliers, lead suppliers and any other parties contributing to the service. Part 1, Clause 4.2 covers the validation of a supplier's process, procedures and documentation for all processes, including configuration management.

Financial asset management

Financial asset management falls outside the scope of the 20000 series, although it is recommended that the service provider should define the interface between configuration management and financial asset management.

Key point

It is useful to map the types of CI used by configuration management to the asset types used in financial management. This helps to align and integrate the two processes. Not all CIs are financial assets but all assets will be CIs or composed of CIs. For example, a process is a service asset, but is not a financial asset.

Configuration management planning

The configuration management plan is part of the service provider's overall service management plan, described in Chapter 4. There should be a current configuration management plan for the management of all CIs. The plan may cross-refer to other documents, e.g. configuration management process and procedures.

An auditor can review the plan as the first step in auditing change and configuration management. This can involve checks to ensure that the two processes are integrated.

Typical roles involved in configuration management are:

- manager responsible for the quality of the process (often the 'process owner') ;
- CI owner/custodian, e.g. for a service, for local assets;
- configuration management architect/designer;
- configuration analyst;
- configuration administrator/configuration librarian.

Generic roles are also used as well, e.g. developer, implementer. Each role is linked to a set of activities and usually to a stage in the lifecycle of CIs.

Configuration identification

Configuration identification ensures that there is a common set of configuration information as the basis for managing, operating and supporting the services. The definition of CIs and each CI's components may be documented in a policy. CIs are usually classified by type and each type is linked to a standard lifecycle, as shown in Table 16.

Table 16 – Examples of CI lifecycles by CI type

CI types	Example lifecycles for CI types				
Service	Accept-ance test	Pilot	In-service	Retired	
Hard-ware	Ordered	Commis-sioned	Live	In store	Retired
Docu-ment	Draft	Approved	Issued	Super-seded	

Identifying, controlling and tracking CIs

The selection, definition and grouping of CIs aims to get the best balance between the information needs of the SMS as a whole and the cost of keeping the information accurate and current. If the selection of CIs and the way they are related and grouped is too complex, too simple or illogical, the information will be difficult to use and not be effective. A process based on a badly designed set of CIs is unlikely to meet the requirements of Part 1.

Key point

Many managers responsible for configuration management define the services and service components as logically related groups of CIs. This helps to define the ownership hierarchy of CIs.

Part 1 requires the service provider to define what information is to be recorded for each type of CI. This typically includes the following attributes:

- unique identifier;
- CI type;
- description of the CI;

- owner/custodian, e.g. service owner, CI owner;
- status;
- version, e.g. file, build, baseline, release;
- location;
- supplier/source;
- relationship(s) between the CI and other CIs;
- associated requests for change;
- associated problems and known errors;
- related document masters;
- related software masters;
- audit trail.

It is recommended that the attributes that describe the specific functional and physical characteristics of each type of CI are defined, e.g. size, capacity.

Relationships

CIs used by the SMS but which are outside the control of the service provider are usually identified by information such as 'X is used by Y'. It is advisable for information held on this type of CI to make it easy to identify who does control these CIs.

Configuration management also defines the documentation for CIs, providing information for other processes. For example, impact analysis and root cause analysis of problems by problem management.

Typical relationships used in the identification of CIs are:

- parent;
- child/comprises;
- used/used by;
- made of;
- connected to;
- installed in;
- impacts/impacted by;
- request for change – affected CI/version;
- request for change – implemented CI/version;
- known error – CI/version that caused a problem.

Examples include a PC that is the parent CI and other CIs are components of the PC. The components will be shown in the next level of the hierarchy. Service providers should be aware that maintaining details of too many relationships will incur costs without bringing additional benefits for control.

Defining configuration documentation

The characteristics of a CI can be documented. For example, a service requirements specification and an SLA for a service can describe the characteristics of a CI of type 'service'. Many organizations specify mandatory and optional documents that describe a CI. Examples are shown in Table 17.

Table 17 – Types of CI and examples of related documentation

CI type	Examples of related information for a CI
Customer contract	Service requirements specification SLA
IT service	Service specification SLA Interface definition Contact list
External suppliers service	Contract SLA (contract schedule) Supplier's service management plan Process interface definition Contact list Shared data environment
Application	Release policy Requirements specification Design specification Release acceptance test plan Technical environment specification Release acceptance test report Release documentation Release software 'Release to production' baseline Licence master documentation
Application installation	Application licence Application installation record

Auditable markings

It is recommended that configuration information should include auditable markings or other methods of identification for CIs. This identifier is then recorded in the CMDB. For each type of CI an auditor can seek evidence of:

- naming conventions;
- data definitions;
- the way the physical or electronic component is labelled;

- physical location of the CI.

It is important to identify the information to be recorded at each state in a CI's lifecycle. Often configuration information is updated when a CI is moved to the next state. The correct level of configuration information detail is important for configuration management to be effective. If the information is too detailed then resources will be wasted in maintaining unnecessary information.

If the level of detail is not sufficient there will be a lack of control and a lack of the visibility required for effective service management.

Configuration baselines

Part 1 requires a baseline of CIs to be taken before a release of CIs is deployed into the live environment. The baseline should be useful for verification audits of CIs, e.g. if a configuration baseline of the software already installed is recorded before new software is released, this can act as the basis for comparison of the configuration before and after the release. This configuration baseline also enables a change or release to be reversed correctly or a service to be recovered in the event of a disaster.

The role of the CMDB

Part 1 includes a requirement that every CI can be identified and that its details are recorded in a database, commonly referred to as the configuration management data base (CMDB). In smaller organizations, a set of spreadsheets might be all that is required for a 'fit for purpose' CMDB. However, even if spreadsheets are adequate it is not acceptable for there to be duplicated or conflicting data in different spreadsheets.

Key point

Financial asset management might only need to know how many of each type of item there are for accounting purposes. Service management also needs to know where they are, how they fit in with everything else, what changes have been made to them and what changes are planned.

At the organization level, the data for CIs used across the organization will often be maintained in a primary database. This may be supplemented by linked databases that hold the details for specific types of CIs, e.g. software, desktop and/or network. Where databases are linked, a portal should be provided for staff to easily find the configuration information and carry out updates.

Figure 10 shows an example of a primary CMDB and related databases. The primary CMDB has the master records for services, service components and high-level CIs and links to the lower level databases. Records for definitive copies of the service and service management documentation are in the service management primary database. These have hyperlinks to the organization's document management system. Automatic updates are received from the human resource, finance and procurement and development configuration management systems.

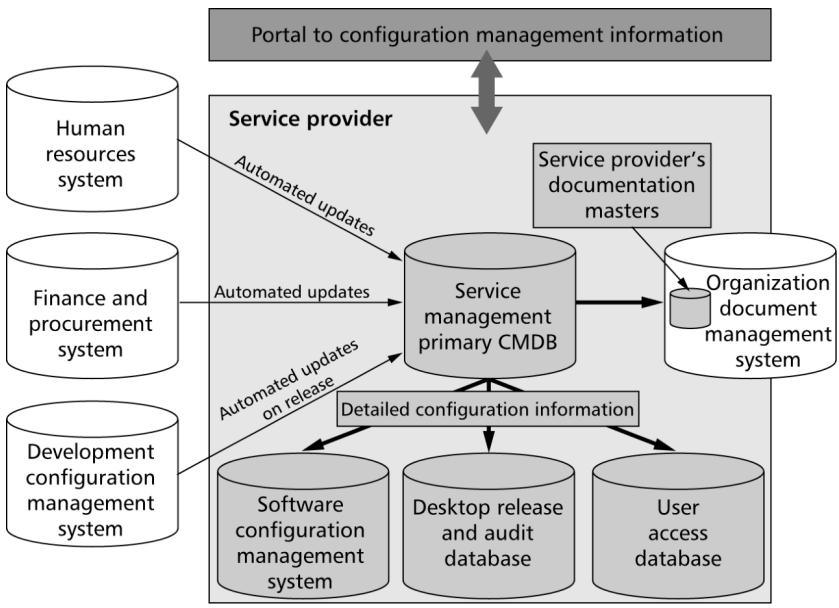


Figure 10 – Example CMDB

The portal to the configuration management system would provide different views of information in the CMDB for people to perform different service management activities. For example, SLM would use a report of the service catalogue, change management would use impact assessment reports and status reports of changes.

Maintaining accurate data and information that is easy to use is important for effective control. An auditor would normally interpret inaccurate or conflicting data as evidence that the configuration management process is ineffective.

Physical and electronic libraries

Part 1 requires that master copies of CIs, such as software and documentation, which are usually referred to as digital CIs, are controlled in secure physical or electronic libraries. References to the libraries are included in the CMDB.

Electronic libraries include both software libraries and document libraries. Physical libraries include hard copy storage such as fireproof safes or filing cabinets.

Although physically separate from the rest of the CMDB, these electronic and physical libraries form part of a single logical repository of configuration information. It is important that staff can quickly locate the definitive versions of software and documentation for use in service management.

The CMDB records references to the definitive version of the document or software object in the relevant library. A 'document library' may be a cupboard that contains hard copy versions of master documents such as contracts and software licences.

Access controls

Many of the service provider's staff require access to the CMDB for their role in service management. This information should be protected during access, e.g. from unauthorized creation of CIs or unauthorized changes to CIs. Other controls can be required, such as preventing access to personal information used to update the CMDB. Access controls vary depending on the type of activity, e.g. creating, changing or removing a CI. For example, staff can be given the correct level of access to the CMDB by control of the hardware, software, media and documentation.

An auditor will not seek evidence of a specific method of access control but will expect to see that the controls are appropriate and that there are no loopholes, such as staff that have changed roles retaining their original access rights.

Key point

It is best practice to standardize and define the roles that are responsible for updating information at each stage of a CI's lifecycle and for change records. Many configuration management tools use this mechanism to ensure that only appropriate staff can update the information at certain points in the process.

Checking information to identify and then correct errors in the CMDB is described in more detail in the sections on 'Configuration control' and 'Status accounting'.

Controlled hardware

Although not specifically required by Part 1, it is usually advisable for hardware CIs to be held in controlled storage areas. Sometimes these are called the definitive hardware store. They are typically used for:

- hardware to be protected from damage or tampering;
- PCs required for controlled builds;
- important spares that can be needed at short notice, e.g. business-critical server.

Configuration control

It is a requirement of Part 1 that the integrity of systems, services and service components is maintained by procedures controlling CIs. Configuration control enables this by ensuring an authorized person updates the information in the CMDB as changes are made to CIs, e.g. changes in the status, location, ownership and version.

Staff need to be clear on exactly what control procedure to apply in particular circumstances. For example, there can be different installation procedures for different computing platforms and staff need to select the right procedure to follow.

Only authorized CIs should be accepted and recorded from receipt to disposal.

Automation

CMDB, version management or library management software is commonly used to produce audit trails of document and software changes.

Many service providers use a configuration management system that provides functions to:

- manually update data, typically with validation of input data;
- automatically update data, e.g. baseline the CIs in a release;
- automatically update data from external tools.

Other tools that are commonly used to automate the configuration management are:

- build tools;
- baseline and comparison tools;
- installation and de-installation tools;
- discovery and audit tools;
- detection of nonconformities and recovery tools.

It is usually advisable that these tools and configuration control procedures automate updates to CI records/CMDB wherever possible. This generally increases the accuracy. For example, when a desktop release is made to 25,000 users, if a desktop distribution tool is used it should automatically update the CMDB when installation on each user's desktop has been completed satisfactorily.

Status accounting

Status accounting of CIs provides the audit trail of changes to a CI as it progresses through its lifecycle, e.g. ordered, in stock, live, disposed. It also ensures that the status of CIs is visible to all those that need the information and is required by Part 1.

The information for status accounting includes information about any uniquely identifiable CI throughout the lifecycle of that CI. It includes the capture, storage, retrieval and access of information necessary to account for the configuration of a service, the infrastructure or constituent CIs. The information is captured in the CMDB. An audit trail is established when a CI is first changed and the audit trail is then updated after each subsequent change.

Configuration management provides information to the status accounting activity. It also includes baselines such as:

- 'as-specified' configuration;

- 'as-designed' configuration;
- 'as-released' configuration;
- 'as-installed' configuration.

It is recommended that the service provider should be able to collate the status of CIs that together constitute a:

- service, configuration or system;
- change, baseline, build or release;
- version or variant of a CI.

To achieve this it is sometimes necessary to baseline the CIs and place the baseline report under the control of the configuration management process.

Status accounting information demonstrates that the service provider is in control of its CIs by providing evidence such as:

- CIs are traceable;
- CIs are auditable by configuration management;
- information on CIs is available to change management;
- a baseline of CI data was captured before the deployment of a release.

Information for other processes

Key point

Configuration management reports play an important role in the service provider's planning, decision-making and support activities by the service provider. For example, the information in the reports is used by personnel, customers, projects and suppliers.

An auditor can ask for details of the way information on reports from configuration management is used by other service management processes.

Reports that provide evidence of the integration of configuration management with other processes include:

- the latest status of CIs with related documentation and version history;
- a list and status of CIs affected by a change;

- a list and status of problem reports and known errors related to the affected CIs;
- the number of changes for each service, environment or CI type;
- an audit trail of changes made to a CI, e.g. changes in the status, location, owner;
- a list of CIs at a physical location or business unit, e.g. in preparation for an audit;
- a list of software versions in the master software library, versions and status;
- a baseline of the appropriate CIs before a release to the live environment;
- a baseline comparison report, e.g. acceptance test and production;
- a release comparison report, e.g. Application X release 2.1 and 2.2.

The service reporting requirements of Part 1, Clause 6.2 also apply to the reports that are produced by the configuration management process.

Configuration audit

Configuration verification and audit activities are used to review CIs to check that the actual CIs match the CIs documented. An objective of a configuration audit is to ensure that software and intellectual property used by the organization is properly licensed and used in accordance with the terms and conditions agreed with the supplier.

The verification and audit activities also check:

- that CIs meet their required attributes and conform to their specification;
- that physical configurations are protected and have not been corrupted;
- that physical configurations match the details recorded in the CMDB;
- that the intellectual capital of the organization is protected;
- the completeness and correctness of the CMDB against the actual;
- the completeness of changed CIs;
- there have been no unauthorized changes.

Many service providers perform audits on samples of CIs. This is a cost-effective approach that will be acceptable for a Part 1 audit if the service provider can demonstrate that the sample is statistically sound and is therefore representative of all the CIs that are the subject of the audit. Nonconformities should be recorded and assessed with input provided to a plan for improving the service.

Configuration audit scheduling

The configuration management process owner is responsible for ensuring that configuration audit activities are scheduled.

An audit plan and/or schedule is usually documented in, or referenced from, the overall configuration management plan. Audits are typically carried out to an agreed timetable, e.g. before and after major change and by sampling at random intervals.

Scheduling of both physical and functional audits is recommended. Often both types of audit are done at the same time, e.g. before an application release.

An example of the types of configuration audits for software assets is shown in Table 18. In this example, the schedule of configuration audits aims to ensure that commercial software assets and the associated licences are accurate. A rolling audit is scheduled for three locations that are given the abbreviations L1, L2 and L3, across each quarter of the year, i.e. Q1, Q2, Q3 and Q4.

Table 18 – Extract from a configuration audit schedule

Audit and frequency	Configuration audit activity	Q1	Q2	Q3	Q4
Software asset verification – Quarterly	Reconciliation between what is installed on each platform and what was authorized for installation, including exceptions identified	L1 L2 L3	L1 L2 L3	L1 L2 L3	L1 L2 L3
Software licensing compliance – Quarterly	Reconciliation between licences owned and required for software used. The basis for and calculations of effective licences	L1 L2 L3	L1 L2 L3	L1 L2 L3	L1 L2 L3
Software asset verification – 6 monthly	Verification of the inventory of software (originals, definitive master versions, builds and distribution copies)	L1 L2	L3	L1 L2	L3
Hardware and platform verification – 6 monthly	Verification of the hardware and platform inventory including locations	L1 L2	L3	L1 L2	L3

Chapter 16 Change management

Introduction

This chapter describes the features of the change management process that ensure changes are assessed, approved, implemented and reviewed in a controlled manner.

The Part 1 requirements for change management can be summarized as:

- CIs to be controlled under this process are defined in a policy;
- all requests for changes are clearly defined, recorded and classified;
- changes are assessed for their risk, impact and business benefit;
- changes are authorized, approved, checked;
- changes are implemented in a controlled manner;
- changes are scheduled and co-ordinated;
- emergency changes are managed;
- unsuccessful changes can be reversed or remedied;
- all changes are reviewed for success and any actions taken after implementation;
- change records are analysed for input to service improvement planning.

What is effective change management?

Change management oversees and co-ordinates the impact assessment, approval, build, test and implementation of a change. The characteristics of effective change management are:

- changes have a clearly defined scope;
- there is a value in delivering the change;
- changes are delivered successfully, on time and within budget;
- no unauthorized changes;
- changes are grouped and packaged for efficient implementation;
- changes are planned – there are few unplanned and emergency changes;
- close co-ordination with customers, projects, development and suppliers;
- changes do not cause problems;
- the process is efficient and so does not cause unnecessary delays;
- staff understand the process and can follow it easily;

- only relevant people are involved at each stage of change;
- clear authorities and responsibilities exist at each stage of managing a change.

Effective change management is responsive to business needs and priorities. This can be achieved by having a single change management process covering business and IT changes, although this is not always possible when the customers and service provider are different organizations.

Change and configuration management should be integrated so that when a change is proposed accurate information on configurations is available. This ensures that the correct CIs and versions are deployed into the correct environment. A request for change should identify the CI(s) that will be affected by the change. As changes are implemented the configuration management information is updated.

Change management policy

Part 1, Clause 9.2 requires a change management policy to be established that defines:

- CIs that are under the control of change management;
- criteria to determine changes with potential to have a major impact on services or the customer including the removal or transfer of a service to another party.

The definition of an emergency change is often included in the change management policy. Many service providers include a clause in the change management policy that invokes disciplinary action if an unauthorized, unrecorded change is made. Many service providers include the requirement to use a documented procedure to record, classify, assess and approve requests for change.

Many service providers use classification criteria based on the potential risk and impact to service. This is useful for controlling small changes that may have a high risk of impacting service. Requests for change classified as having the potential to have a major impact on the services or the customer are managed using the design and transition of the new or changed services process. The requirements for this are in Part 1, Clause 5. All other requests for change to CIs defined in the change management policy are managed using change management. In practice, these processes work together and a service provider should define when each process should be used in the policy.

Some requirements in Part 1, Clause 9.2 depend on the definition of an unsuccessful change. It is useful for the change management policy to include a definition of successful or unsuccessful change. Some service

providers use a category of 'partially successful' and this would need a clear definition. For example, a deployment or a software release to 99% target users can be considered successful if there is a procedure to update the remaining 1% of users.

Recording all changes

Recording all changes ensures that:

- there is a full audit trail of changes;
- change records can be analysed;
- the impact of changes planned at the same time can be assessed;
- reporting is useful and consistent;
- all the costs associated with changes are understood, e.g. for each service.

An auditor can ask the management team about their role in preventing unauthorized change. Evidence that there is management commitment to preventing unauthorized change may be in the form of records such as those on disciplinary action taken when an unauthorized change has been made.

There can be national legislation or an organizational policy that constrains the use of personal information in this way, in which case an auditor would seek alternative evidence of management commitment.

Configuration audits can provide evidence of whether all changes are recorded and controlled by the change management process. Audit activities produce a report of errors in the configuration data or the actual CIs and can help to identify process nonconformities.

Unauthorized changes can be identified by using this information. For example, problem management can identify an unauthorized change after requesting a configuration audit to identify the root cause of failure for:

- downtime;
- a major incident(s);
- an increase in incident volume;
- problems and errors.

Classifying different types of change

Part 1 includes a requirement that all requests for change are classified (e.g. urgent, emergency, major, minor) enabling changes to be prioritized and managed.

The classification is usually based on features of the change:

- scale of the change;
- potential impact if the change fails;
- risk that the change will fail;
- benefits of making the change;
- risk and impact if the change is not made;
- timetable for the change;
- person or people who will agree the change;
- the need to make a change in an emergency.

Typical examples are shown in Table 19.

Table 19 – Example classifications for changes

Classification	Description	Examples
Change model or change type	Determines workflow for different types of change	Pre-approved, normal, emergency
Risk	Risk to the business and the IT services	High, medium, low
Business impact	Impact on the organization. May be combined with change category to determine approval	High, medium, low Global, regional, country, site
Priority	Priority to be used in scheduling the change	Critical, high, medium, low
Change category/ change authority	Determines which people need to be involved with reviewing and approving the RFC	Minor, significant, major

Change management lifecycles/models

For greater efficiency, different types of change may follow a different lifecycle and have different workflows, i.e. the classification is used to determine which procedure is used for managing the change. For example, a low risk 'routine' change has a proven method for implementation, is simple and will have little impact if it does fail. Typically, budgetary authority is given in advance, based on a cost agreed in advance. The change manager is usually responsible for deciding which changes can be implemented as routine changes.

In contrast, a normal change has a longer lifecycle than a pre-approved change. The risks and impact of the normal change are given more attention than a routine change.

It is good practice to ensure that the stages of the change lifecycle for each type of change are consistent across the organization. This avoids misunderstandings on who does what and when it is done, which can result in changes failing or conflict between changes to be done at the same time.

Table 20 shows common relationships between type of change and a lifecycle.

Table 20 – Examples of lifecycles for different types of change

Category/class	Example lifecycles for CI types
Pre-approved	Raised, assigned, closed
Normal	Raised, impact assessment, approved, scheduled, implemented, reviewed, closed
Emergency	Raised, approved, reviewed, closed
New service	Plan, design, develop, transition via release and deployment, operation

Emergency changes

It is important to plan the way emergency changes will be managed before the emergency arises. By their nature, emergency changes are higher risk than if there were time for consideration of each aspect of the change. Unless emergency changes are planned for, the process can degenerate into confusion and result in a worsening of the situation.

Part 1 requires that the service provider and the customer agree the definition of an emergency change. This can be achieved by the customer agreeing to the emergency change definition that is referenced from an SLA. Part 1 also requires the service provider to use a documented procedure for managing emergency changes.

Key point

It is recommended that the usual change management process is followed as far as possible for emergency changes. Some steps may be completed later or documented retrospectively, e.g. independent testing. It is also common for the same stages to be followed but for each stage to be accelerated.

Because emergency changes present a high level of risk, Part 1, Clause 9.2 requires the service provider to have emergency change policies, processes and procedures to control the authorization and implementation of emergency changes. An auditor could check whether the use of the emergency change process complies with the definition of an emergency, or whether the emergency change process is used for changes that should and could have been scheduled in advance.

Roles in change management

One of the challenges that service providers face is understanding the customer's and supplier's organization when planning changes, e.g. roles, responsibilities, authorities, accountabilities and approval levels of individuals for changes. Effective control of changes requires clarity on roles and responsibilities for all stages of the change lifecycle, e.g. who has the authority to approve each type of change?

Part 1 does not specify the way this should be documented. One method is to obtain this information from the configuration management process as the information about the owner/custodian of affected CIs should be available for each CI or CI type.

Change initiator

Initiating a request for change is a key interface between change management and customers, projects, developers, suppliers and the other service management processes. It is important that the change initiator has appropriate authority to raise a request for change and sufficient information to clearly define the proposed change.

Change manager

The change manager usually has overall responsibility for change management on an operational, day-to-day basis. This person has responsibility for ensuring that the process is established and that the agreed process is followed, including the correct classification being chosen for changes and the correct people authorizing each change. This person does not normally have any involvement or responsibility for changes actually being made, nor responsibility for the actual recording of changes.

This person may also be the change management process owner, i.e. the person responsible for the quality of the process itself. Some service providers separate the responsibility for the process on a day-to-day operational basis from process ownership. The change manager in a large

service provider or one that is making many changes may have a team, often combining the change and configuration management processes.

The typical responsibilities for a change manager include:

- ensuring that requests for change are classified correctly;
- approving changes that do not need to be approved by a change authority;
- chairing a change advisory board;
- scheduling changes with advice from the change authority;
- overseeing building, testing, implementation and back-out of changes;
- co-ordinating audits and reviews of changes.

Change authority

The authorization for a change is often linked to the classification of the change, so that for each type a different level of authority applies.

Formal approval is obtained from people often referred to as a change authority. The change authority may be an individual but commonly the role is shared by several people. Many service providers link authority levels for changes to monetary values such as the estimated cost of the change. For example, large changes that affect several distributed sites might need to be approved by a higher level change authority such as a global change board or even, in exceptional circumstances, a board of directors.

A group of people who have collective authority for approving changes are often referred to as a change advisory board.

Other change management roles

The change manager is often supported by one or more change administrators who are actively involved in the process, normally on a day-to-day operational basis.

Other roles involved in the change management process are typically:

- change developer/builder – supplier of the change, e.g. project or external supplier;
- independent tester, e.g. a tester who is independent of the change builder;
- change implementer – person who implements the change into the environment.

Identifying and recording requests

Part 1 requires that requests for change have a defined scope. This requirement can be fulfilled by clearly stating information such as the purpose of the change, the affected service, service components and/or CIs, the impacted customers, impacted users together with their business unit and location.

Good quality information should be held for each clearly defined service, service component and/or CI. Having a link between the change and what the change will affect ensures that the whole process works efficiently.

To support the Part 1 requirement that requests for change are assessed for their risk and impact, certain types of change should include information to support the assessment, as described in the next section. To support risk assessment, a service provider should include a plan of the activities required to reverse or remedy an unsuccessful change. For example, the risk and impact of a change that can be reversed quickly with no impact on the service will be different to a change that needs to be remedied by invoking a service continuity plan.

Key point

Requests for change should be written in appropriate language for the target audience to understand, e.g. business language for customers and technical language for the service provider's own staff.

If a change is badly documented a reliable impact assessment is not possible. Missing or misleading information can result in the impact assessment being based on incorrect assumptions, leading to incorrect conclusions and a failed change.

Assessing risk and impact of proposed changes

Part 1 requires that all requests for change are assessed for their risk, financial impact and potential impacts to:

- services and the customer;
- service requirements;
- business benefits;
- technical feasibility;

- other services.

Information from change management and other processes support the assessment. Configuration management provides information for impact assessment, such as a list of the potentially affected CIs and the owner or custodian of the related service or service component. This helps to understand dependencies and to identify interested parties to consult during the assessment of proposed changes.

The impact analysis will depend on the scale and type of change. The person responsible for the change or the CI that is to be changed and all parties that will be affected are identified and asked to contribute to an assessment of the risk, financial impact and potential impacts.

As many affected parties can be involved, the risk is often assessed from multiple perspectives and a consensus might need to be reached on the way to mitigate risk. For example, assessing risk from the business or customer perspective can result in a different set of actions than assessing risk from an IT perspective.

The detail recorded for an impact assessment depends on the type of change and the assessment technique used. For example, a major change may require a detailed impact assessment to be recorded. In contrast, a minor change may be documented by a few sentences in the main body of the request for change.

If many people are involved in impact assessment, it is usual to summarize the overall views in the body of the request for change clearly so staff can understand the impact of the proposed change. The detailed impact assessments would still be available as well.

Many service providers implement an impact assessment procedure based around a standard form or screen so that all aspects of the impact assessment are included.

Budgeting and accounting practices provide the mechanisms for predicting and tracking the costs of a change to quantify the business benefit of the change.

The change management process owner is responsible for ensuring that impact assessment, including any forms or screens, is suitable for good management decision-making on change approvals.

Assessing changes in relation to each other

Proposed changes also need to be assessed in relation to one another and against the existing planned schedule of changes. This ensures that the full impact of each change is understood before the change is

scheduled avoiding a clash between two separate changes. For example, by looking at the changes that are targeted for a weekend the impact assessment can identify a clash between two changes because of the order or timing. Batching changes also saves effort and costs.

A service provider should identify the risks associated with doing too many changes in the same time period if there are dependencies or limited resources.

Scheduling changes

Scheduling is an important activity that enables the service provider to respond to real business needs and demands by planning the implementation of changes that maximize business benefit ahead of other changes.

Key point

Part 1 requires that the scheduled implementation dates of changes are used as the basis for scheduling changes including the deployment of releases. This means that changes that are already scheduled for specific time slots (often called change windows) are not moved unnecessarily. If implementation dates are changed it is important that impact assessment and approval is repeated.

The approved and scheduled changes are typically documented in a plan, schedule or change calendar that is then used in planning further changes and deployment of releases.

Part 1 requires that a schedule of planned change is established and communicated to all interested parties. Many service providers do this by making the plan accessible via the intranet. The Internet may be used if suppliers at remote locations are involved.

The advantage of publishing the schedule of planned changes is that those responsible for implementing the change can try to schedule their changes at times that do not affect other previously planned and scheduled changes.

If there are many changes, it is usual to break down the schedule of planned changes by service and/or geographical area affected.

Some service providers adopt change freezes when the risk of a change, however well managed, is not acceptable, for example, in periods of unusually important business activity, or immediately before a major service or infrastructure change.

Decisions on the acceptance of requests for change

The culture of a service provider's organization will influence the manner in which decisions are made on the acceptance of requests for change. Hierarchical structures for authorizing changes can impose many levels of change approval, while flatter structures can allow a more streamlined approach.

Similarly, the culture of the customer's organization influences change management, particularly for organizations that are not predisposed to follow standards or processes unless forced to do so.

Some organizations prefer to concentrate authority onto a small number of people, whilst others prefer a large committee structure for decision-making.

Part 1, Clause 9.2 requires that the service provider and interested parties make decisions on the acceptance of requests for change. Decision-making takes into consideration the information from the assessment of risks, the potential impacts to services and the customer, service requirements, business benefits, technical feasibility and financial impact, discussed in previous sections in this chapter. An important aspect is to ensure that the appropriate people and interested parties are involved in making the decisions.

Key point

Authority levels for proposed changes can be linked to values such as the estimated cost of the change or levels of impact and risk. The levels of authorization can be linked to the classification of the change, so that for each type a different level of authority applies. For example, large changes that affect several distributed sites might need to be approved by a higher level change authority. In exceptional circumstances this could be a board of directors.

Whatever approach and criteria are used for the acceptance or rejection of requests for change, an auditor can request evidence of the approval

process and will assess the effectiveness of this. Evidence of interest to the auditor can be a sample of requests for change records that record the decision or minutes of a meeting where the decision was taken.

Staged approval

Many organizations approve changes in stages, where one stage has to be approved before the next. This is the case particularly for changes that will ultimately incur significant costs. Examples of staged approval are the following sequence:

1. resources to assess and define the requirements for a change;
2. resources to design a change and review (often done as part of a project);
3. resources to build and test a change (often done as part of a project);
4. implementation of a change into a controlled environment (e.g. acceptance test);
5. deployment of a release in the live environment;
6. resources to provide early life support until service acceptance is agreed.

This may be tracked on one or more requests for change.

Change approval or rejection

The change authority role considers the business benefits and recommends whether the change should be approved for development and testing, approved for deployment or rejected.

Changes that require approval for deployment into the acceptance test or production environment need to have a scheduled implementation date and time otherwise the impact cannot be assessed.

If changes are rejected it is important that the change initiator is notified of the decision and the reason for the decision so that they can reconsider and replan. The role of the change initiator is described earlier in this chapter in the section on 'Roles in change management'.

Developing and testing changes

Part 1 requires that approved changes are developed and tested. Failing to implement an approved change can cause a later change to fail if there was a dependency. For whatever reason, changes that are not developed and tested should be notified to change management and another impact assessment should be performed.

The classification of successful and unsuccessful change is important to be able to demonstrate that the Part 1 requirements have been met. If a change is deemed to be unsuccessful then the activities required to reverse or remedy the will be performed. This should be carried out according to an agreed plan that has, where possible, been tested. For example, if an application software release has to be backed out because a script failed part way through deployment it is important to be able to back out of the change and leave the IT service in a known configuration. Part 1 requires that CMDB records are updated following the successful deployment of changes.

Key point

Unsuccessful changes need to be investigated and agreed actions taken. The status of the change, the reason for failure and agreed actions identified during the investigation should be recorded.

Predeployment test

Part 1 requires that changes are tested before deployment. This typically includes:

- testing that authorized changes are properly built and conform to specification;
- testing that changes to CIs can be verified during deployment;
- testing any change back-out or remediation plans in case of failure.

Changes are often deployed by a person belonging to the group that is responsible for or the custodian of the CI being changed. Change management is responsible for:

- co-ordinating the deployment of changes;
- liaising with configuration and release management as appropriate;
- ensuring that there are records with evidence of verification of the change;
- co-ordinating the back-out or remediation of failed changes.

Verifying completion

Change management should verify that the change has been developed and tested in a controlled manner by checking that the change records and configuration documentation are accurate and complete. This can

include a check that the change record is correctly linked to the affected CIs, and the correct version of the implementation and release documentation is issued. The CMDB records shall be updated following the successful deployment of changes.

If required, change management may request a configuration audit of the related CIs from configuration management.

Review and closure

Part 1 requires that all changes are reviewed, after implementation. Different types of change typically require different levels of review.

For some changes, such as a major change, a post-implementation review meeting will be held to review the outcomes. A post-implementation review aims to check that the change met its objectives, that customers are happy with the results and that there have been no unexpected side effects. It is good practice to record lessons learned and feed any improvements into the service improvement programme. The outcomes and actions are reported in the meeting minutes.

For other changes, a summary of a review may be recorded on the change record or a related document, e.g. showing the impact of a change on the number of incidents and problems for the affected CI in the period after the change.

Change management should review all completed emergency changes to:

- check that bypassed steps have been completed;
- check that the documentation is complete;
- verify that the change was a true emergency.

The actual costs, resources and time are usually recorded as part of the review and closure activities.

The change records are closed when all the documentation has been completed.

Analysing changes and inputs to improvements

A proactive aspect of change management is the analysis of changes in order to identify trends and opportunities for process improvement. Part 1 requires change records to be analysed regularly to detect trends, e.g. increasing levels of changes, frequently recurring types, emerging trends and other relevant information. The results and conclusions of the analysis need to be recorded to meet the requirements of Part 1.

The change management process owner is responsible for scheduling regular analyses and ensuring that the results and conclusions are recorded.

Typical examples are:

- increase in volume of changes by CI type and/or owner;
- variation in actual versus estimated cost/resource/time;
- volume and frequency of changes against success over time;
- improving the lead time from raising a change request to implementing the change;
- maximum/average/minimum time for each step in the workflow by type and/or category of change.

All processes in service management and the PDCA cycle place a high level of importance on continual improvements to the quality of the service. An auditor will expect to see evidence of the information from the analyses, results and conclusions being used in identifying opportunities for improvement.

Chapter 17 Release and deployment management

Introduction

This chapter describes the key features of the release and deployment management process that delivers, distributes and tracks new or changed service components in a release into the live environment.

The requirements can be summarized as follows:

- a release policy is agreed with the business and all relevant parties;
- releases, pilots and deployments are planned well in advance;
- acceptance criteria for the release are agreed with the customer and interested parties;
- resources are co-ordinated during release and deployment;
- the release and build mechanisms ensure the integrity of service components, including hardware and software, during deployment;
- releases are built and tested in a controlled acceptance test environment prior to deployment;
- unsuccessful releases can be backed out or remedied;
- the success and failure of releases is monitored, measured and analysed;
- provision of inputs to the change management process for planning and impact assessment;
- provision of inputs to service improvement.

The release and deployment process

The process is used to group a set of related and compatible CIs, known as a release, and deploy them into the live environment. Typically, this means a group of changes are made to a set of CIs using a consistent, repeatable method.

Typical circumstances where the release and deployment management process is the most advantageous approach are:

- introduction of a new or changed service;
- changes to a desktop build (hardware and software);
- applying a desktop application across many PCs;

- release of a new or changed service to many users;
- distribution of a maintenance package of fixes or repairs;
- release of an application;
- refresh of a technology or other major upgrade;
- keeping software current, e.g. security patches;
- tracking the deployment of software assets and licences.

Key point

Each release and deployment is governed by a request for change raised via change management. This ensures that the group of changes in a release are assessed for impact, authorized, scheduled and deployed correctly.

Release and deployment management also ensures that the changes in each release are compatible with each other and that none clash with other unrelated changes.

What is effective release and deployment?

Release and deployment management should be integrated with configuration and change management. It is important to be clear on the scope of release and deployment management because the process crosses organizational boundaries. Release and deployment management should also have a holistic view of changes, ensuring all aspects of a release are considered together.

Careful planning ensures that there is no ambiguity about what tasks are included in release and deployment management, what is included in other processes and the way processes interface to any projects providing a release.

All changes and CIs in a release are tracked via interfaces to change and configuration management. This level of control also helps the service provider achieve compliance with statutory, regulatory and contractual requirements related to the management of intellectual property rights, assets and software licences.

Figure 11 shows the key relationships between release, change and configuration management processes.

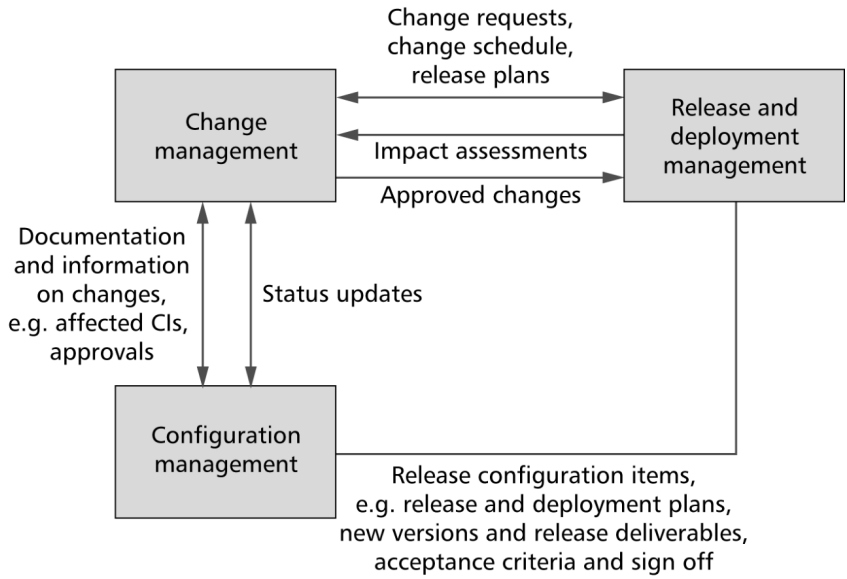


Figure 11 – Relationship between the three processes

Benefits of release and deployment

Release and deployment management can provide benefits such as significant cost savings and better control. This is often achieved by:

- grouping related changes into a release for efficient implementation;
- standardizing the release and deployment activities;
- automating release and deployment (once there is a standard method);
- removing unnecessary approval steps and handoffs;
- reducing manual actions that cause errors and inconsistencies;
- changing the frequency of releases to maximize resource utilization;
- phasing deployment to improve the impact on customers and users.

Effective release and deployment management results in:

- higher success rate in delivering new and changed services;
- reduced risk to the business;
- no waiting time or rework;
- few back-outs;
- a successful deployment across the user base on time and to budget;
- cheaper and streamlined process that all parties understand;
- all CIs involved in a release are traceable and auditable;
- improved staff, customer and user satisfaction.

Stages of release and deployment

Release and deployment management covers the main aspects of:

- planning the release;
- development of a release to meet customer and service provider's needs;
- deploying the release to target locations, business units, users or platforms.

Key point

Care should be taken to ensure release management does not work in isolation. This is bad practice and causes issues. Projects should use release and deployment management.

The process provides an independent and integrated interface with the rest of the SMS. This is irrespective of whether the team implementing the release also produces the release or is another team.

It is recommended that a release:

- complies with the appropriate standards;
- meets the requirements of the business and customer;
- meets the service provider's requirements;
- addresses operational issues and risks;
- is deployed with suitable notice to those involved or affected with communication and training.

Information on operational issues, such as incidents, is passed to the team that produced the release, for correction or classification as a known error.

The release policy determines the way the release is planned and defined as the first stage of the process. This is then followed through to the acceptance test stage. After successful acceptance the release is deployed under agreed plans. The final stage is a review of the effectiveness of the release.

At all stages there is integration with the project, team or external supplier that is the source of the release. Updates are fed back to the change and configuration management processes.

Release policy

A release policy helps to set expectations on the nature of a release and when a release will be more appropriate than a series of separate changes. The policy states the frequency and type of releases.

The following are recommended additions:

- definition of each type of release including an emergency release;
- identification schemes for releases;
- roles and responsibilities for release management;
- authority for the move into acceptance test and production environments;
- rules for unique identification and description of all releases;
- approach to grouping changes into a release;
- agreed approach to automating to aid repeatability and efficiency, e.g. pull versus push deployment;
- identification of the release and deployment approach;
- identification of the testing approach;
- rules on verification and acceptance of a release.

The role of release manager

Key point

Understanding the release policy means that all those involved in the deployment of a release are also able to plan and budget for resources well in advance. It is therefore essential that someone with sufficient authority and responsibility for the release and deployment management process works with an equivalent manager involved in the service level management process. This person is required to define the approach and agree this with the relevant parties, such as the customer.

The managers who need to work closely together have roles that are commonly referred to as the 'release manager', 'deployment manager' and the 'service level manager'. A typical release manager is involved in the process on a day-to-day basis. This includes ensuring that the process is followed and that records and plans are updated in the correct timescales and with the correct information. An example is given in Table 21.

Table 21– Roles and responsibilities for a release

	Design and development	Pre-acceptance test	Acceptance test	Acceptance test	Live
CI type	Released from	Released from	Accepted by	Released from	Accepted and supported by
IT service	Service designer	Development manager	Transition manager	Release and deployment manager	Service level manager
Central appication	Development manager	Configuration manager	Test manager	Configuration management	Support manager
Database schema	Development manager	Development manager	Database administrator	Configuration management	Database administrator
Physical database	Development manager	Development manager	Database administrator	Configuration management	Database administrator
Infrastructure	Environment manager	Environment manager	Operations and support manager	Configuration management	IT operations manager
Personal computers	Logistics	Environment manager	Desktop support	Configuration management	Desktop support
Desktop build-new release	Development manager	Configuration manager	Desktop support	Configuration management	Desktop support
Desktop installation	Environment manager	Environment manager	Desktop support	Configuration management	Desktop support
Release authorization	Development configuration manager	Configuration manager	Test manager	Stated in release policy and approved by change management	Business operations and IT service desk

Other roles involved in release management

There are other roles involved in release and deployment management, so the accountabilities and responsibilities should be clear as the release moves from the development and test stages into the production environment. The configuration management process assists with this by documenting the scope of the release management roles, accountabilities and responsibilities for each CI type during the release and deployment cycle. Configuration management is described in Chapter 15.

Accountabilities and responsibilities also need to be clear for changes that have the additional protection of Part 1, Clause 5. These are changes that have the potential to have a major impact on the services or the customer. There should be no ambiguity about 'who does what and when' at all stages. The person with the roles of transition manager or release and deployment manager will work closely with the person with the role of service owner or service level manager to ensure that the transition completes successfully.

Frequency of releases and deployments

Reducing the frequency of releases can reduce disruption to the live services significantly, and also reduce overheads associated with managing releases. However, this might not be acceptable to fast moving businesses where speed-to-market is essential and the business requires daily updates.

Different parts of the customer's business may also have different needs, each needing to be managed individually. For example, a marketing department can require a release and deployment every day whereas a financial department may prefer one every quarter. The policy, process and procedures also need to cater for emergency releases.

Key point

There can be a significant impact on the customer's business, service provider and suppliers if the frequency of releases is inappropriate. Working with the SLM process minimizes the risk of inappropriate frequency being used.

Release and deployment approach

Planning will depend on the type of release being developed and the deployment approach.

Typical examples that require a different approach are:

- new service to target business units, customers, users, platforms;
- desktop release to target computers and users;
- mainframe application to target business units, customers, users;
- security patch by platform.

Different types of change can be grouped into one release if the amount of change involved can be handled by the service provider and its customer's business. However, if many independent changes are grouped into a release it can be difficult to manage the dependencies. If too few changes are grouped into a release then the overhead can be excessive and inefficient.

Agreeing an approach

The approach for the type of release needs to be agreed with the customers and interested parties. One option may be to perform consecutive releases with all users upgraded. Another option may be to pilot before the full deployment. The latter starts the planning for the next release once the previous release is in pilot. This provides the opportunity for more frequent releases.

In distributed environments, it is often lower risk to pilot a release at a few locations before rolling out an application, e.g. in one country before deployment is done globally. It is also common practice to freeze the contents of a release at a fixed interval before the release is implemented.

For all new and changed services subject to Part 1, Clause 5, the plan should be developed as more information is obtained, providing a better understanding of the most appropriate way of releasing and deployment. For example, if a detailed deployment plan is developed nine months in advance there are likely to be differences to the contents, the environment that will receive the release and, in particular, the customer's business needs.

Release definition

Part 1 requires the release documentation to record:

- release identification, which follows naming and numbering conventions;
- whether the release is an emergency release;
- the associated deliverables for a release and deployment;
- the deployment dates;
- method of deployment;
- related requests for change that are to be implemented;
- known errors that are fixed;
- new known errors or problems in the new release;
- acceptance criteria.

A good configuration management system will help the service provider to keep track of the relationships between records. For example, the records that are created to track the requests for change for a new release and the related CIs. Configuration management provides information about these documents, the relationships between them and the status of each change and CI.

Release management may check key criteria, for example:

- the release has a clearly defined scope;
- relevant business objectives, policies, requirements and plans are identified;
- the service requirements are unambiguous and can be tested/measured;
- outcomes from operating a new service are expressed in measurable terms.

Release and deployment planning

Part 1 requires the service provider to plan with the customer and interested parties the deployment of new or changed services and service components into the live environment. Planning should be co-ordinated with the change management process and include the dates for deployment of each release, the associated deliverables and the methods of deployment.

It is best practice for the plans for the same type of release to contain the same basic activities each time, because a consistent approach is easier to manage.

Typical considerations for planning are:

- scope and content of the release, including deliverables;
- time and resources needed to package, build, test and deploy a release;
- services and service components to transfer, decommission or remove, including licences;

- timetable for the deployment of the release;
- roles and responsibilities for building, testing and deploying the release;
- the release and deployment procedures and methods;
- communications planning activities;
- approach to identify, track and manage issues detected;
- test plans;
- approach to managing controlled test environments;
- approach to managing assets according to applicable policies;
- criteria that the release and deployment should be verified against;
- approach to back out of or remediation for an unsuccessful deployment and testing such plans.

Approving and communicating the plans

Part 1 requires that the deployment plans are agreed with the customer and all interested parties. This can be achieved by using a request for change for the deployment of a release, ensuring that all relevant parties will be informed.

Key point

Resolution management staff should be aware of the plans for the release and deployment so that they can be prepared, e.g. training staff so they can answer queries after the deployment of a release.

Developing or acquiring software

It is recommended that software releases should be checked by configuration audit activities. Any software versions and other electronic files should be stored in configuration management and the relevant secure library.

Designing, building and configuring a release

The release and distribution mechanisms need to be designed to ensure that the integrity of hardware and software and other service components are protected at all stages. It is best practice to:

- use standard release management procedures and tools;

- reduce manual steps that are error prone and costly;
- ensure that software licences can be managed and authorized;
- ensure that software licences will be redeployed where appropriate;
- ensure a release can be backed out of or remedied if unsuccessful;
- manage components using software libraries and related repositories;
- ensure the target platform satisfies prerequisites before installation;
- check a release for completeness when it reaches its destination;
- check that the build complies with the architecture and standards.

Part 1 includes neither requirements nor recommendations for automation of deployment and distribution tools. However, some form of automation is normally beneficial as it can reduce costs and the risks of a mistake being made.

Controlled acceptance test environment

Part 1 requires the service provider to establish a controlled acceptance test environment to build and test all releases prior to deployment into production. The type of evidence that an auditor might seek is:

- configuration baseline report of the acceptance test environment;
- configuration baseline report of the production environment prior to release;
- gap analysis on the acceptance test environment baseline and production environment;
- configuration baseline report of the production environment after the release.

Key point

The controlled acceptance test environment does not need to be a dedicated physical environment. For example, a service provider might not have an acceptance test environment but have a maintenance time slot that allows enough time to use the production server for the acceptance test prior to installing the release.

This is acceptable as long as there is a well-tested back-out or remediation plan should there be any issues.

Release acceptance

The change management process requirements given in Part 1, Clause 9.2 require that new or changed services are accepted by all relevant parties, e.g. the customer, stakeholders, service provider staff and suppliers. It is important to base formal approval on the results of the acceptance test using agreed acceptance criteria before deployment. Proactive service providers will ensure that the release requirements are addressed during the design and development of the release.

If the acceptance criteria are not met, the service provider will need to take a decision on necessary actions and subsequent deployment activities with interested parties.

CIs for a release

It is recommended that all associated updates to documentation should be included in the release, e.g. business processes, support documents and SLAs.

Additional examples of CIs and documentation that would be under configuration management at the acceptance test and release-to-live stage are:

- release definition and requirements so changes are made against these;
- environment configuration baseline, e.g. acceptance test;
- application configuration baseline and release;
- training plan for service management, support staff and customers;
- communications plan(s);
- test plans;
- back-out/remediation and contingency plans;
- service management documentation (if new or changed service);
- support documentation, e.g. support procedures and administration instructions;
- build, release, installation and distribution processes and procedures;
- known error list;
- release note(s);
- evidence of acceptance testing;
- evidence that the release is ready for release to live.

The three stages below provide examples of acceptance checks that a service provider can perform at the design and acceptance stages when implementing a release (using configuration management verification and audit procedures).

Stage: Release Design and Build

- Service and release requirements can be delivered by the release design
- Assets in the release are designed to meet regulatory requirements and contractual obligations
- The build and release mechanisms for deployment are efficient and effective
- Training plans and communication mechanisms are planned
- The acceptance test plan can test the requirements and design criteria
- The acceptance criteria can be tested

Stage: Before testing in the controlled acceptance test environment

- The communications plan ensures all parties involved know about the release
- Training is planned and for staff and users to be involved in acceptance testing
- Service and CI documentation is under configuration management
- The CMDB, supporting systems and tools have been updated

Stage: Before and during deployment into live

- Evidence that testing in the acceptance test environment is completed and the acceptance criteria have been met
- Release documentation is complete and under configuration management
- Deployment plan(s) are accepted by all relevant parties (if applicable)
- Communications plan ensures all parties know about the release and deployment
- Staff and users are trained and ready
- Sufficient support resources have been planned (link to capacity management)
- All release and deployment deliverables are under configuration management
- Each deployment is accepted by the relevant parties before final handover

Deployment of a release

Having established plans for the release, the release is deployed in a way that ensures that the integrity of hardware, software and other service components is maintained at all stages.

This is dependent on:

- the type and size of the customer's business activities;
- the number of users/locations (and time zones);
- associated system type and size;
- other releases or changes that are also occurring;
- the quality and currency of configuration management information;
- the availability (or otherwise) of tools for the automation of the process.

Unsuccessful deployment

The activities required to reverse or remedy unsuccessful deployment of a release should have been planned and tested. Unsuccessful releases need to be investigated and agreed actions taken.

Updating information

The release management process should include the updates to configuration information throughout the deployment. The change management process assesses the impact of requests for change on releases and plans for deployment. Information about the success or failure of releases and future release dates is required by the change management, incident and service request management processes.

Post-deployment

Part 1 requires the service provider to measure the success or failure of releases by measuring the incidents related to a release following deployment. This includes analysis of the impact on the customer, business, IT operations and support staff resources. This is typically input into the post-implementation review of the release or associated change.

Feedback should be given to the post-implementation review for the corresponding change request. The results and conclusions drawn should be used to identify improvements, such as fixes for the next release.

Chapter 18 Design and transition of services

Introduction

This chapter describes the requirements in Part 1, Clause 5 for new and changed services starting at the design stage, going through the transition stage and ending once the service is fully operational and stable.

Organizations are constantly changing. There are many different types of business change, including major changes such as business improvements, legal and regulatory changes, mergers, acquisitions and divestitures. A service provider that is capable of making changes quickly and reliably for their customers and business provides significant business advantages.

A service provider needs to understand the existing services and the environment within which existing services operate in order to understand the risk and impact of changes. All changes carry some risk and risk assessment and risk management are essential to delivery of service. The correct and balanced application of the Part 1 SMS will minimize risk without incurring an excessive overhead either before or after changes are made.

Changes that could have a major impact

The need for a new service or a change to a service can originate from the customer, the service provider, an internal group or a supplier in order to satisfy business needs or to improve the effectiveness of the services.

Part 1 includes requirements for managing types of changes that by their nature are high risk or have a major impact. Examples include changes that will have a widespread impact, such as the deployment of a new version of desktop software to thousands of users. Other examples include changes to a system used by a small number of people that, if it fails, could be life-threatening.

The three control processes, configuration, change and release and deployment management, are at the core of managing all changes to the

SMS and services. They are fundamentally proactive and essential to an SMS. However, sometimes, even these three processes are not enough. Changes that have the potential to have a major impact on the services or the customer can require the extra protection of Part 1, Clause 5. These types of change are normally a project or programme of projects that interface to the SMS, with Part 1, Clause 5 defining the way that interface should be managed.

Not all changes, not even all big changes, require the additional protection of Part 1, Clause 5. A change management policy, a requirement in Part 1, Clause 9.2, should include criteria that define the type of changes to which Clause 5 applies. Each service provider may have different views on the most appropriate criteria. For example, a change affecting more than an agreed number of users, or more than an agreed percentage of office locations could be part of the criteria. Any change that could put the service provider at risk of being penalized under data protection legislation or regulations on proof of financial probity could be other forms of criteria. Part 1, Clause 5 requires that removal or transfer of a service is always classified as a change with potential to have a major impact and therefore should always have the added protection of Clause 5.

Key point

When a service provider contracts a new supplier there can be a higher than usual risk. The higher risk can continue until the supplier is fully aware of the way the service provider operates and the service provider's routine expectations of their suppliers. With a new supplier, smaller, lower-risk changes can be given the additional protection of Part 1, Clause 5. Once the supplier has a proven track record it is acceptable to dispense with the additional requirements of Clause 5. In this case, the supplier is managed using the requirements for governance in Part 1, Clause 4.2. The service provider will also apply the requirements for supplier management in Part 1, Clause 7.2. This will include appointing an individual to be responsible for managing the relationship, the contract and performance of the supplier.

Role of the control processes

The service provider should ensure that the service requirements, plans and design, once accepted, should be progressed in a well-managed and

timely manner. As well as Clause 5, the control processes in Clause 9 have an important role. For example, the service requirements and design will be composed of CIs already in use or that will be acquired as part of the development of the service.

The CIs, which are the building blocks used for the development of the new service, should be under the control of the change and configuration management processes, as well as the planning, development and implementation control provided by Part 1, Clause 5. New CIs should be added to the CMDB as they are used in the development, so that they can also be controlled.

Key point

Most changes that require the additional protection of Part 1, Clause 5 requirements are a series of interrelated changes. These should be managed and deployed as a release, or possibly more than one release.

The first step

The service provider should make the criteria to meet the requirements for Part 1, Clause 5 changes clear to programme and project management, established suppliers, potential suppliers, and their own managers and personnel. This is essential because Clause 5 starts with the very earliest stage of a new or changed service and getting involved later can be too late.

Identification of the need for a new or changed service can originate from many different groups and for many different reasons. It can start as a service provider-led initiative, but can also come from the customer, an internal group working closely with the service provider, or a supplier. The reasons for a new or changed service can be varied as well, e.g. business needs, improving efficiency, gaining competitive advantage or even protection from the threat of legal action.

Getting the service provider involved after the service has been planned and designed is too late for optimal risk management. Being involved late leaves the service provider with less time to plan and prepare. This is especially the case if there are other changes planned for the same time that could create an unacceptable overall risk. The nature of other changes could mean that both changes cannot be done at the same time, however important they might be.

So who plans and designs?

A service provider may opt to plan and design all their new and changed services themselves. This is probably the simplest way to interface projects to the SMS, because all managers and personnel involved are under the direct control of the service provider. However, these are rare circumstances – like many other aspects of the SMS, there are normally other parties involved who are outside the direct control of the service provider.

New or changed services may involve several different groups, perhaps each with a specialism required for a large and complex service. Finalizing decisions on who is involved requires careful co-ordination and an assessment of the relative benefits, costs and risks of different supply models.

Example – major change and interfacing with projects

An organization suffered significant issues during periods of major change. The results were poor quality services that cost more to deliver and use than originally estimated. Although the service provider had established the Part 1 control processes, project changes were not in scope of the SMS. Often, the service provider was not engaged early enough with each project. Notification of project changes and releases were usually late, increasing the risks of change.

The service provider worked with the project management office, an internal group, to establish clearly defined interfaces, review and handover points throughout the service lifecycle. The authority, responsibilities and communications were defined between all interested parties, including customers and external suppliers. The service provider's top management agreed the engagement and communication mechanism with projects. Top management mandated the interfaces between projects and the control processes. Service owners became accountable for service acceptance.

Adopting service lifecycle practices and meeting the Part 1, Clause 5 requirements for the design and transition of new and changed services enabled the service provider to reduce failed project changes whilst improving the estimated cost of changes. It allowed the service provider to maintain, control and have visibility of the state of its services and components.

Planning for design and transition

In simple terms a good plan delivers what is needed, when it is needed, at the quality expected and at the cost agreed.

A key step is to identify the service requirements for the new or changed services. These should be agreed by the service provider, customers and any interested parties. Further information on service requirements is provided in the next section. Meeting the agreed service requirements then becomes a key goal during planning of new or changed services, influencing what is planned and the way it is planned.

The plans can be complex and should take into account a diverse range of factors, all of which can affect the SMS, e.g. funding for the planning, design and development, transition into operational running. The cost of operation should be considered and built into the budget. The way the cost of operation should be paid for is also required for the accounting process, e.g. will costs be allocated or apportioned, as described in Chapter 11.

A new service can also require organizational changes, such as a new specialist support group, different staffing levels and skills, different working hours or shift patterns. Interim support arrangements can be considered advisable for the first few weeks of operational running, and this and the eventual transfer to normal support services need to be planned for in advance.

The technical impact of a new or changed service should be considered, e.g. the risks from the service to SLAs, changes needed to the service catalogue, extension of a customer satisfaction survey to cover the new service and, if relevant, the new users of the new service.

Capacity management will be required to model the impact of the new service on performance, projecting workloads so that the capacity plan can be adjusted and if necessary hardware, software and other resources upgraded.

Key point

The service provider needs also to plan for removing services. Planning includes the date(s) for the removal, archiving, disposal or transfer of data, documentation and service components, including licences.

Planning for the new or changed services should contain or include a reference to at least the following:

- authorities and responsibilities for design, development and transition;

- activities by the service provider and other parties including activities across interfaces from the service provider to other parties;
- communication to interested parties;
- human, technical, information and financial resources;
- timescales for planned activities;
- identification, assessment and management of risks;
- dependencies on other services;
- testing required for the new or changed services;
- service acceptance criteria;
- expected outcomes from new or changed services, in measurable terms;
- any improvements to the effectiveness of the services.

The service provider should identify other parties who will contribute to the provision of service components for the new or changed services and evaluate their ability to fulfil the service requirements.

The results of the evaluation need to be recorded and necessary actions taken.

Identifying service requirements

Part 1 defines a service as a means of delivering value to the customer by facilitating results the customer wants to achieve without the ownership of specific costs and risks. This definition sets a focus for delivering new or changed services under the requirements of Part 1, Clause 5.

The design of a new or changed service should be based on the needs of the people who will use the new service and those that operate, support and improve it. There is after all no point in delivering a service if it has basic flaws that mean it is unreliable to use or results in someone being prosecuted.

In Part 1, service requirements are based on the needs of the customer, users of the service and the service provider. They also include the interested parties of the SMS such as internal groups and suppliers.

The service requirements need to be clearly defined because they are used as the basis of the service acceptance criteria.

Key point

The business requirements should be considered as inputs when identifying the service requirements.

Examples of business requirements include:

- vision and mission strategies;
- changes to the context, scope and cost of use of the service;
- corporate governance, statutory and regulatory requirements;
- contractual obligations;
- information security management objectives;
- human, financial, organizational and technical constraints.

Within the context of the business requirements, the scope of the service requirements should cover a service in use and the way the service is to be delivered.

Requirements for a service in use include what the service is, why it would be used, when it is appropriate to use the service and where the service can be used. These requirements are used to design the service. Part 1 includes the following requirements that need to be identified:

- scope and description of the new or changed service to be delivered;
- desired results to enable value delivery for the customer;
- how and where the service will be used, e.g. customers, business units;
- forecast demand for service;
- changes to the customer's capabilities and resources required to use the new or changed service;
- known limitations that constrain the use of the service;
- service level requirements to meet specifications including service targets, workload characteristics and exceptions.

The service provider has a key role in defining the way the service is to be delivered. This includes the way the service provider's assets – both capabilities and resources – will be used to plan, establish, implement, operate, monitor, review, maintain and improve the service. Part 1 includes the following requirements for a new or changed service and any changes required for the SMS:

- service continuity and availability requirements;
- capacity and performance requirements;
- information security requirements;
- authorities and responsibilities between service provider and customers;
- contractual obligations;
- new or changed human resource requirements, including requirements for appropriate education, training, skills and experience;
- changes in financial arrangements;
- reporting and communication mechanisms.

What is a good design?

A good design of a service solution needs to meet the business and customer requirements within a particular context of use, whilst being comprehensive and complete. Missing an element of service provision from the design can result in a funding shortfall or risk to service provision.

Early designs can be created in a burst of enthusiasm with ideas such as functionally rich systems, a high level of automation and use of emerging technology. The service provider might need to bring reality to the discussions by explaining that the ideas are not as easy as first thought, or too costly.

Key point

All interested parties need to be brought into the discussions early to ensure that the design of the solution is accepted by all those involved. Typical issues at this stage include: will the service actually run in an operational environment? Will it be possible to support it cost-effectively?

A structured approach to service design helps to ensure that the new or changed service will be developed and transition into operations within planned timescales, quality criteria and at the right cost.

Designing the service in use should include:

- changes to SLAs, contracts and other agreements to align with changes in service requirements;
- updates to the catalogue of services;
- consideration of existing technology and architecture;
- activities to be performed by the customer and service provider;
- changes to support new or changed human resource requirements, including appropriate education, training, skills and experience;
- reporting and communication mechanisms.

Designing the way the service is to be delivered should include:

- activities to be performed by each party;
- changes to the SMS;
- new or changed plans and policies as required by Part 1;
- procedures, measures and information for operation of the services;
- assets and licences to provide the service;

- financial resource requirements for delivery of the new or changed services;
- new or changed technology to support the SMS;
- all acceptance criteria.

Assessing the impact

In Part 1, the service provider is responsible for determining and providing the human, technical, information and financial resources needed to enhance customer satisfaction by delivering services that fulfil service requirements. Therefore, the service provider needs to take necessary actions to ensure that the new or changed services can be developed and transition effectively into operational use.

A useful step is to use a checklist for assessing the impact of new or changed services. An example is given below.

Checklist for new or changed services

Part 1 requirement – Example of assessment questions

Impact on the customer

- Will the service meet the business and customer expectations, requirements and desired results?
- What are the risks in using the service?
- Is there any impact on the customer's organization, customer's existing policies, processes or procedures?
- Is there a good communication plan?

Impact on services

- Are there implications for existing services, e.g. SLAs, formal agreements, services, contracts?
- Can the service levels be measured?
- Is the service aligned with the IT architecture?
- Are standard services and configurations used?
- What are the risks to existing services?
- Can the expected results from the service be measured?
- Is there any impact or risk of not doing the change?

Impact on finances

- Is the estimated total cost of ownership acceptable?
- Has the budget been updated to reflect the change to the service management, operations and support?

- It there an impact on the existing cost of running the service change, e.g. extra staff for handling incidents?
- Is a higher volume of incidents expected during first months of operation and how will this be funded?
- Are there any more opportunities for reducing costs?

Impact on human resources

- Is there any impact on capacity and staff, e.g. do our staff have the right skills and experience?
- Do we need to reorganize the teams to deliver the service?
- Is there an impact on the service provider staff? For example, do staff need to move locations, work different hours?

Impact on service management framework

- Does the change affect the scope of service management, e.g. by increasing the customer base or supported locations?
- Is there an impact on existing policies, processes, procedures, documents and records?
- Does the service comply with corporate governance, legal and regulatory requirements?
- Is it aligned with the service management scope, plans and requirements for delivering efficient and effective services?
- Can the service be managed and controlled across the supply chain?

Impact on technology

- Does the new or changed service introduce new technology? If so, is there a plan to introduce the new technology?
- Is the new or changed service based on standard architectures, standard configurations and standard builds?
- Is the impact on capacity defined?

Impact on supplier management

- Are the supplier management requirements and constraints addressed?
- Is there any additional impact on supplier management, contract management and their interfaces?
- Have suppliers been assessed for their capability to support and control the new or changed service?
- Have any contract changes been identified?

Are planning and design outputs acceptable?

Part 1 requires the service provider to review outputs from the planning and design activities against the agreed service requirements. Based on the review, the service provider should accept or reject the outputs.

It is important for enough time to be made available for appropriately skilled personnel to assess the outputs from the plan and design activities, well before proposals are finalized. The review should include reaching a view on whether the plans and design are expected to meet the agreed service requirements.

Key point

In badly managed projects, the service requirements might not be considered until after the plans and design for a new service have been proposed. For example, focus could have been on new functionality, use of novel technology or to get a service to market as quickly as possible with no thought to long-term consequence. The people involved might not have realized how important it is to design a service so that it will actually meet service requirements and not just provide sophisticated functionality.

The review should also cover how effective the actual planning has been – does the plan include timescales, dependencies, roles and costs? Is there enough detail to know what will be delivered when? Can the proposals be checked against service requirements or have they not been produced rigorously enough?

Any risks or uncertainty should be followed up and resolved promptly. It is inevitable that all changes involve some risk, but significant risks should be understood and accepted if they cannot be removed by improvements to the design or plans.

If it is not possible to resolve issues that represent an unacceptable risk to the new service or the existing service, the plans and design should be rejected. The assessment and rejection of the design and plans can all too easily become a source of time-wasting and counterproductive conflict. To avoid this, the final judgement on the plans and design should be made against objective and measurable criteria. The criteria should be agreed with the project, in advance. The decision will still be very unpopular with those making the new service proposals, but at least it will be clear on what basis this decision has been made.

Checklist: planning and design

a) Has it been agreed who will have decision-making authority at each stage of the planning and design?
b) Are the service requirements acceptable?
   - Have all the service requirements been identified, documented and formally agreed?
   - Do the requirements cover the needs of customers and the service provider?
   - Do the service requirements include the service levels, continuing support skills, hours, workloads, capacity?
c) Have all the service impacts been considered and are they acceptable?
   - Is it clear what role will be played by the customers and users of the prospective service?
   - Have the customers accepted the projected service levels and costs, including the cost model for apportioning any shared service costs?
   - Have the implications for the service catalogue, SLAs and service continuity been judged acceptable?
   - Will any new contracts or changes to contracts (and other documented agreements) be required to support the new service?
d) Are the changes to the SMS acceptable?
   - Have all changes to the SMS been identified and formally agreed?
   - Have new or changed procedures, measures and information to be used for operation of the new or changed services been identified?
   - Are changes to policies, processes and procedures acceptable?
e) Are the plans comprehensive and acceptable?
   - Are there any major clashes in the timetable, e.g. an office relocation at the same time as a key stage in the new service implementation?
   - Has the role of the Part 1, Clause 9 control processes been considered and allowed for in the plans?
   - Are the numbers, skills and experience of support staff understood and allowed for in the plan – and will the budget cover this?
f) Have all the costs been included and are they acceptable?
   - Has the cost of the project (plus contingency) been included in capital budgets for the year the costs will be incurred?
   - Have the costs of the implementation and immediate post-implementation support been included in budgets?
   - Have the costs of continuing support been estimated, discussed, agreed and included in budgets?
g) What is the proposed supply model and is it acceptable?

- In-house by the service provider?
- Using external skills managed by the service provider?
- Multiple suppliers managed by the service provider?
- A single lead supplier managing sub-contractors?

h) Is the service provider organization engaged and ready?
- Are the service provider's own managers and personnel aware of what is involved?
- Is everyone clear about who is responsible for what – especially themselves?
- Will the service provider's personnel be able to manage the service with the proposed supply model?
- Will the change, release and deployment plans fit with the service provider's other work?
- Is it clear what role will be played by other parties, for example internal groups that will contribute but are not in the scope of the SMS?

i) Are the acceptance criteria OK?
- Have acceptance criteria been developed by the service provider and do they cover the key risks to the service?
- Do the acceptance criteria cover both functionality aspects as well as performance aspects of the new service?
- Is everyone clear on the way the acceptance criteria will be used and who has the authority to use them?

Transition of new or changed services

Before actual implementation of the service it is essential that the service is tested in a safe environment, where any defects cannot affect the actual operational service.

Test plans should be designed to check that the actual service developed meets the service requirements originally agreed.

If the design has been well done and carefully checked before development and the service has been developed according to the agreed design, the service should operate as expected.

It is essential to have built the expected features into acceptance criteria to use during testing. This not only makes the testing stage more effective and faster, but it means everyone involved understands in advance what is acceptable, and what is not. Rejection of the service if it does not meet the acceptance criteria is not then a shock to any of those involved.

Key point

Service acceptance criteria are most effective when worded in objective and measurable terms. For example, the rate of faults, support service levels, speed of response for an online system and overall support costs are all examples.

In reality, acceptance tests results are not usually all perfectly met or all completely failed. Most are a mixture of acceptable results and lower quality than required, e.g. more faults than expected or slower performance than the design indicated would be achieved. At this time a round of discussions is almost inevitable, in which options for improving defective features are debated. Almost inevitably this will also involve changes to expected costs and possibly the budgets for future years.

During the transition of a service, the release and deployment process is used to deploy changes into the live environment. Part 1, Clause 9.3 requires that the success or failure of releases is monitored and analysed. The results and conclusions drawn from the analysis of a deployment should be recorded and reviewed to identify opportunities for improvement.

Review for effectiveness

As for any large project or programme it is necessary to review the strengths and weaknesses of the project, the actual outcomes compared to the expected outcomes. The strengths and weaknesses from the project and the interface to the SMS should be considered for lessons learned.

With changes of this scale and nature a wide range of managers and personnel will have a need to know the results of the review. The service provider needs to report the outcomes to interested parties.

Appendix A Terms and definitions

The following are taken from Part 1, Clause 3, with some formatting changes. For example, NOTES have been incorporated into the actual definition. All other words in the 20000 series are used in the normal English language sense.

3.1 Availability – ability of a service or service component to perform its required function at an agreed instant or over an agreed period of time. Availability is normally expressed as a ratio or percentage of the time that the service or service component is actually available for use by the customer to the agreed time that the service should be available

3.2 Configuration baseline – configuration information formally designated at a specific time during a service or service component's life. Configuration baselines, plus approved changes from those baselines, constitute the current configuration information. Adapted from ISO/IEC IEEE 24765

3.3 Configuration item (CI) – element that needs to be controlled in order to deliver a service

3.4 Configuration management database (CMDB) – data store used to record attributes of configuration items, and the relationships between configuration items, throughout their lifecycle

3.5 Continual improvement – recurring activity to increase the ability to fulfil service requirements. Adapted from ISO 9000:2005

3.6 Corrective action – action to eliminate the cause or reduce the likelihood of recurrence of a detected nonconformity or other undesirable situation. Adapted from ISO 9000:2005

3.7 Customer – organization or part of an organization that receives a service(s). A customer can be internal or external to the service provider's organization. Adapted from ISO 9000:2005

3.8 Document – information and its supporting medium. From ISO 9000:2005
EXAMPLE Policies, plans, process descriptions, procedures, service level agreements, contracts or records. The documentation can be in any form or type of medium. Documents, except for records, state the intent to be achieved

3.9 Effectiveness – extent to which planned activities are realized and planned results achieved. From ISO 9000:2005

3.10 Incident – unplanned interruption to a service, a reduction in the quality of a service or an event that has not yet impacted the service to the customer

3.11 Information security – preservation of confidentiality, integrity and accessibility of information. In addition, other properties such as authenticity, accountability, non-repudiation and reliability can also be involved. Adapted from ISO/IEC 27000:2009

3.12 Information security incident – single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security. From ISO/IEC 27000:2009

3.13 Interested party – person or group having a specific interest in the performance or success of the service provider's activity(ies). A group can comprise an organization, a part thereof, or more than one organization EXAMPLE Customers, owners, management, people in the service provider's organization, suppliers, bankers, unions or partners. Adapted from ISO 9000:2005

3.14 Internal group – part of the service provider's organization that enters into a documented agreement with the service provider to contribute to the design, transition, delivery and improvement of services. The internal group is outside the scope of the service provider's SMS

3.15 Known error – problem that has an identified root cause or a method of reducing or eliminating its impact on the services by working around it

3.16 Nonconformity – non-fulfilment of a requirement. From ISO 9000:2005

3.17 Organization – group of people and facilities with an arrangement of responsibilities, authorities and relationships. The arrangement is generally orderly. An organization can be public or private EXAMPLE Company, corporation, firm, enterprise, institution, charity, sole trader, association, or parts or combination thereof. From ISO 9000:2005

3.18 Preventive action – action to avoid or eliminate the cause or reduce the likelihood of occurrence of a potential nonconformity or other potential undesirable situation. Adapted from ISO 9000:2005

3.19 Problem – root cause of one or more incidents. The root cause is not usually known at the time a problem record is created and the problem management process is responsible for further investigation

3.20 Procedure – specified way to carry out an activity or a process. Procedures can be documented or not. From ISO 9000:2005

3.21 Process – set of interrelated or interacting activities which transforms inputs into outputs. From ISO 9000:2005

3.22 Record – document stating results achieved or providing evidence of activities performed. From ISO 9000:2005
EXAMPLE Audit reports, incident reports, training records or minutes of meetings

3.23 Release – collection of one or more new or changed configuration items deployed into the live environment as a result of one or more changes

3.24 Request for change – proposal for a change to be made to a service, service component or the SMS. A change to a service includes the provision of a new service or the removal of a service which is no longer required

3.25 Risk – effect of uncertainty on objectives. An effect is a deviation from the expected – positive and/or negative. Objectives can have different aspects (such as financial, health and safety, and environmental goals) and can apply at different levels (such as strategic, organization-wide, project, product and process). Risk is often characterized by reference to potential events and consequences, or a combination of these. Risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated likelihood of occurrence. From ISO 31000:2009

3.26 Service – means of delivering value for the customer by facilitating results the customer wants to achieve. Service is generally intangible and can be delivered to the service provider by a supplier, an internal group or a customer acting as a supplier

3.27 Service component – single unit of a service that when combined with other units will deliver a complete service. A service component can consist of one or more configuration items
EXAMPLE Hardware, software, tools, applications, documentation, information, processes or supporting services

3.28 Service continuity – capability to manage risks and events that could have serious impact on services in order to continually deliver services at agreed levels

3.29 Service level agreement (SLA) – documented agreement between the service provider and customer that identifies services and service targets. A service level agreement can also be established between the service provider and a supplier, an internal group or a customer acting as

a supplier. A service level agreement can be included in a contract or another type of documented agreement

3.30 Service management – set of capabilities and processes to direct and control the service provider's activities and resources for the design, transition, delivery and improvement of services to fulfil the service requirements

3.31 Service management system (SMS) – management system to direct and control the service management activities of the service provider. A management system is a set of interrelated or interacting elements to establish policy and objectives and to achieve those objectives. The SMS includes all service management policies, objectives, plans, processes, documentation and resources required for the design, transition, delivery and improvement of services and to fulfil the requirements in this part of ISO/IEC 20000. Adapted from the term quality management system in ISO 9000:2005

3.32 Service provider – organization or part of an organization that manages and delivers services to the customer. A customer can be internal or external to the service provider's organization

3.33 Service request – request for information, advice, access to a service or a pre-approved change

3.34 Service requirement – needs of the customer and the users of the service, including service level requirements, and the needs of the service provider

3.35 Supplier – organization or part of an organization that is external to the service provider's organization and enters into a contract with the service provider to contribute to the design, transition, delivery and improvement of services or processes. Suppliers include designated lead suppliers but not their sub-contracted suppliers

3.36 Top management – person or group of people who direct and control the service provider at the highest level. Adapted from ISO 9000:2005

3.37 Transition – activities involved in moving a new or changed service to or from the live environment

Appendix B 20000 series

Part 1 contents

The numbers in brackets are the number of words/number of requirements ('shalls') for each clause or subclause. Part 2 has the same structure as Part 1.

Foreword (322/0)
Introduction (540/0)
1. Scope
1.1 General (241/0)
1.2 Application (228/0)
2 Normative references (65/0)
3 Terms and definitions (1329/0)
4 Service management system general requirements
4.1 Management responsibility (338/4)
4.2 Governance of processes operated by other parties (160/4)
4.3 Documentation management (303/8)
4.4 Resource management (142/3)
4.5 Establish the SMS (1119/42)
5 Design and transition of new or changed services
5.1 General (218/7)
5.2 Plan new or changed services (293/11)
5.3 Design and development of new or changed services (216/3)
5.4 Transition of new or changed services (114/5)
6 Service delivery processes
6.1 Service level management (234/11)
6.2 Service reporting (166/5)
6.3 Service continuity and availability management (349/18)
6.4 Budgeting and accounting for services (164/5)
6.5 Capacity management (146/6)
6.6 Information security management (362/14)
7 Relationship processes
7.1 Business relationship management (222/14)
7.2 Supplier management (375/12)
8 Resolution processes
8.1 Incident and service request management (263/14)
8.2 Problem management (160/9)
9 Control processes
9.1 Configuration management (295/15)

Part 3 contents

Part 4 Contents

Part 5 Contents

Appendix C Example audit evidence

This should not be taken as a complete list of what will be required during an audit. The auditor can ask for additional supporting information and can use alternative names for documents or records.

Policy, process and procedure for each process
Input to a plan for improving the service
Clause 4.1 Management responsibility
Service management policy and plan
SMS design
Communication procedures
Communication records
Risk assessment reports
Risk management reports
Framework to establish and review service management objectives and policy
Defined authorities and responsibilities
Appointed management representative
Asset records
SMS performance and opportunities for improvement report
Clause 4.2 Governance of processes operated by other parties
Definition of processes to be operated by other parties
Accountabilities, authorities and responsibilities for process operation
Details of interfaces for processes operated by other parties
Process performance and compliance reports
Priorities and plans for process improvement
Clause 4.3 Documentation requirements
Documents required for planning, operation and control of the SMS
Service management policies and plans
Service catalogue and SLAs
Details of service management processes, interfaces and procedures
Document control records
Evidence of records control

Clause 4.4 Resource management
Resource plans and reports for human, financial and technical resources
Personnel development plans
Evaluation report of personnel development plans
Personnel records of education, training, skills and experience
Clause 4.5 Establish SMS
Service management plan
Allocation of funds and budgets
Assignment records for authorities, responsibilities and process roles
Evidence of management of human, technical and information resources
Risk assessment reports
Risk management reports
Details on methods for monitoring and measuring the SMS and services
Audit programme/plan
Objectives of internal audits
Internal audit reports
Communication records of nonconformities
Report of results of actions to correct or fix nonconformities
Objectives of management reviews
Management review reports
Decisions and actions from management reviews
Continual improvement policy
Continual improvement procedures
Evidence that improvements are managed, from identification onwards
Improvement plan
Measurement of implemented improvements against targets set
Report on implemented improvements
Corrective action if targets are not met
Clause 5 Design and transition of new or changed services
Change management policy on what is included in Clause 5
Risk assessments for new or changed service requests
Plans for all stages of the new or changed services
Plans for retirement of services, as appropriate
Report on assessment of other parties contributing to any stage in Clause 5
Service requirements for new or changed services

Potential impact of delivering the new or changed services
Expected outcomes from delivering the new or changed services
Design of new or changed services
Evaluation of new or changed services fulfilling service requirements
Development of new or changed services verified against the design
Service acceptance criteria developed
Verification of new or changed services against service acceptance criteria
Report on outcomes achieved against expected outcomes following transition
Clause 6.1 Service level management
Service catalogue
SLAs
Agreements with internal groups
Records of reviews meetings with internal groups/customers acting as suppliers
Inputs to and output from reviews of SLM, service catalogue, SLAs
Service reporting requirements
Service review planning activities
Monitoring and control report
Service review records, causes of nonconformities, improvement opportunities
Proposed changes to service requirements, catalogue, SLAs, other agreements
Service improvement plans
Clause 6.2 Service reporting
Report requirements, for all parties
Report design
Report schedule
Reports of performance against targets, corrections and corrective actions
Reports on workload characteristics, performance reporting
Reports on customer satisfaction, complaints, nonconformities
Reports on trends and forecasts
Decisions and actions based on findings in service reports
Process review report
Proposed changes to reports
Clause 6.3 Service continuity and availability management
Service continuity and availability management policies
Service continuity and availability management requirements

Business impact analysis
Risk assessment reports
Service continuity and availability plans
Customer requirements including SLAs and required levels of service
Service continuity plan test report
Availability constraints and data
Test report of availability against availability requirements
Training requirements and records
Assessment of the impact of changes on the plans
Investigation report on unplanned non-availability
Proposed changes to service continuity and availability plans
Clause 6.4 Budgeting and accounting for IT services
Details of process interface with other financial management processes
Policies and procedures for budgeting and accounting
Budgets for previous year
Budgets for current year
Forecasts for next year/draft budgets
Input from other processes, including forecast workloads, planned expenditure
Plans for capital spend in next year
Financial reports of capital and revenue for each time period in the budget year
Reports on financial variance
Reports on the causes of variances/proposed management
Cost models with cost types, rules for cost allocation and apportionment
Legal or regulatory reports
Evidence of financial control and approval
Information to support the costing of requests for change
Clause 6.5 Capacity management
Capacity and performance requirements
Capacity plan
Capacity management baseline and profiles
Capacity threshold and alarm specification
Capacity performance reports
Capacity usage reports
Workload reports and forecasts
Records of performance tuning
Clause 6.6 Information security

Information security management strategy
Information security policy
Information security plan
Physical, administrative, technical security and information security controls
Information security reports
Information security management process effectiveness and efficiency reports
Security risk assessments
Information security risk management report
Information asset inventories
Report on effectiveness of information security policy
Trends in information security incidents
Opportunities for improvement
Clause 7.1 Business relationship management
Details of customer/interested parties, contact information, roles, services
Role of the designated individual to be responsible for each contract
Agenda and minutes of meetings between the service provider and suppliers
Service reports showing overall performance of the service provider
Records of complaints and actions taken
Customer satisfaction survey/measurement and actions
Clause 7.2 Supplier management
Role of the designated individual responsible for each supplier and contract
Supplier contracts
The interface between processes operated by multiple parties
Responsibilities, roles and identities of all parties
Records from periodic contract review meetings
Records relating to lead suppliers managing sub-contracted suppliers
Nonconformities and opportunities for improvement
Clause 8.1 Incident and service request management
Incident records
Service request records
Major incident records
Major incident meetings and action plans
Opportunities for improvement from review of a major incident
Call performance records
Incident escalation records

Reports on volumes and type of incidents and service requests
Statistical reports on call types, closure types, classifications, volumes
Incidents passed to problem management for problem investigation
Clause 8.2 Problem management
Problem records
Known error records
Problem resolutions
Proposed changes to resolve incidents and problems
Problem review input, output and meeting minutes
Trend information
Clause 9.1 Configuration management
Details of process interface with financial asset management
Definition of each type of CI
Configuration management procedures
A list of CIs and their relationships to other CIs
Configuration records
Configuration baselines
Configuration management reports
Configuration audit reports
Clause 9.2 Change management
Change management policy
Requests for change
Impact and risk assessments of proposed changes
Plan to remedy or reverse an unsuccessful change
Schedule of changes
Criteria for Clause 5 changes, in change management
Decisions on acceptance of requests for change
Communication records
Change management reports
CMDB
Trends in changes by volume, type and success/failure
Clause 9.3 Release and deployment management
Release policy agreed with each customer
Definition of a release
Description of the release
Relationship between the release and its constituent CIs
Design, release notes, and installation guides for the release
CMDB
Release and deployment plan

Schedule of releases and deployments
User impact assessment and business change impact assessment
Risk assessment for releases and deployments
Release acceptance criteria
Communications plan on releases
Training plans for new releases
Test plans and test results
Verification of release against acceptance criteria and sign off
Non-conformance report
Records of success and failure with actions
Incident and problem records for release failures, reversals or remediation work
CI information for each release
Release identifier and version
Location of the release package and installation
Associated known errors and problems, including those corrected by the release

Appendix D Case study – creating value

Background

In 2006, a commercial IT service provider signed a contract with a new customer that required the service provider to achieve ISO/IEC 20000-1:2005 within 2 years. A key value driver for the customer was a business and technology transformation programme that aimed to deliver significant cost savings over 5 years.

The journey

The vision for the service provider was to deliver world class IT services that enabled business and technology transformation. The strategy was to implement the processes across the organization. The initial scope for ISO/IEC 20000 would be the customer's business-critical services. The service management objectives were:

- deliver service to the agreed service levels;
- improve customer satisfaction;
- enable effective business transformation;
- simplify services and processes.

A service management programme board was established to direct the implementation.

Year 1

ITIL was selected as the best practice guidance for service management. ISO/IEC 20000 training and the ITIL qualification scheme would be used for the professional development of staff.

A plan for the implementation of service management processes at key milestones was agreed with the customer. The first year milestones included:

- key staff trained in ITIL;

- new service desk established;
- first set of processes established based on ITIL processes:
  - service level management;
  - service reporting;
  - service catalogue management;
  - incident management;
  - problem management;
  - change management;
  - configuration management;
- process owners allocated to ensure that the processes are fit for purpose;
- service owners identified for business-critical services.

The focus for the first year was to manage unprecedented call volumes at the service desk. Initially, the focus was on high priority high volume areas, but as more permanent fixes were implemented the calls reduced by 20% over the first 6 months. The service levels for incident response and resolution times were also achieved.

Many transformation programmes and projects started. As new services were being introduced, a new service catalogue structure was developed. The customer-facing services were clearly separated from the supporting services such as infrastructure and technology services.

Towards the end of the year, the SMS structure was designed including the service management plan, policies, processes and procedures. There was management commitment, clear accountability and a set of key performance indicators for improvement.

Year 2

The plan for the second year was to establish the SMS and extend the set of processes to include the rest of the service delivery processes and the relationship processes. Improving desktop support, email and web services were a key focus for improving customer satisfaction.

Now that staff understood the importance of adopting a process approach, the first year polices, processes and other SMS documentation were revised and simplified. Process documents were standardized using a RACI matrix (as shown in Chapter 6) and they were linked to key performance indicators. The RACI matrix helped to establish the roles with accountabilities and responsibilities for each main activity.

Major changes to IT services became a significant challenge for the operations teams. To cope with this, the service provider used the recently upgraded ITIL service lifecycle practices: strategy, design, transition, operation and continual improvement. Struggling with

transformation challenges, the service provider started using some of the service design and transition practices. This enabled the service provider to achieve the ISO/IEC 20000-1 requirements for planning and implementing new and changed services relatively easily.

The service provider achieved ISO/IEC 20000-1 certification.

Years 3–4

The teams adopted many of the ITIL service lifecycle best practices that enabled major change, including best practices in ITIL service strategy. A key improvement was the introduction of a service portfolio and a customer agreement portfolio. This helped the service provider to understand the big picture – which services were used by which customers, which were new, which were changing and which ones were being retired. This helped the business relationship managers to manage the customer expectations and manage change with their customers better. The operations teams were able to improve their planning and optimize their resource utilization.

Key operational improvements were achieved by implementing the ITIL event management and request fulfilment processes. The self-service channel for service requests from users was popular and delivered significant productivity gains.

Delivering

The customer renewed the contract. The service provider's CEO said:

> *We are now more focused on delivering end-to-end services that create value for our business and our external customers. Investing in developing our service management capability has enabled business transformation whilst maintaining control. Achieving certification to ISO/IEC 20000-1 is good marketing for delivering world class IT services and we are growing our customer base.*

Going forward

The service provider is extending the scope of ISO/IEC 20000 certification and plans to upgrade to ISO/IEC 20000-1:2011.

A key question is, 'What is the impact of moving to certification ISO/IEC 20000-1:2011?' As the service provider has already adopted many of the ITIL service lifecycle best practices this should be relatively easy.

Particular areas where the service provider's adoption of ITIL best practices supports the 2011 requirements are:

- ITIL Service Strategy practices support requirements in Clause 4 and Clause 5, e.g. strategy management, service portfolio management, demand management;
- ITIL Service Design and Service Transition practices support new requirements in Clause 5 and 9;
- ITIL Continual Service Improvement practices support the PDCA requirements in Clause 4.

Bibliography

ISO/IEC 20000-1:2011, *Information technology — Service management — Part 1: Service management systems requirements*

ISO/IEC 20000-2:2005, *Information technology — Service management — Part 2: Guidance on the application of service management systems. To be published*

ISO/IEC TR 20000-3, *Information technology — Service management — Part 3: Guidance on scope definition and applicability for ISO/IEC 20000-1*

ISO/IEC TR 20000-4, *Information technology — Service management — Part 4: Process reference model*

ISO/IEC TR 20000-5, *Information technology — Service management — Part 5: Exemplar implementation plan*

ISO 9000:2005, *Quality management systems — Fundamentals and vocabulary*

ISO 9001, *Quality management systems — Requirements*

ISO/IEC 15288, *Systems engineering — System lifecycle processes*

ISO/IEC 19770-1, *Information technology — Software asset management — Part 1: Processes*

ISO/IEC 27000:2009, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

ISO/IEC 27001, *Information technology — Security techniques — Information security management systems — Requirements*

COOPER, Lynda. *A Guide to the New ISO/IEC 20000-1: The differences between the 2005 and the 2011 editions.* London: BSI, 2011.

DUGMORE, Jenny and Shirley LACY. *A Manager's Guide to Service Management*. 6th ed. London: BSI, 2011.

ITIL®, http://www.itil-officialsite.com/

COBIT® Framework for IT Governance and Control, http://www.isaca.org/Knowledge-Center/COBIT/Pages/Overview.aspx

Introduction to the ISO/IEC 20000 Series
IT Service Management

This book includes guidance on the scope, applicability and implementation of a service management system. It covers the establishment of an SMS, day-to-day operational service and major changes. This enables effective control, delivery and improvement of services that provide value for customers. As personnel need to be well-organized, this book covers some aspects of managing and motivating managers and personnel. It provides easily understood advice on 'what the requirements mean', 'how to do it' and 'what evidence will be required', and will predominantly explain and expand on Part 1 of ISO/IEC 20000. It includes a road map to the second edition of the standard and how it fits in the bigger picture for best practices. Other features include:

- A list of example audit evidence
- *Key Points* boxes, to summarize and emphasize issues of particular importance
- Examples and case studies, to illustrate real-world practice
- Terms and definitions used in the 20000 series.

"This book provides a much needed practical reference for anyone who needs to quickly understand, assess, design and transition service management processes to attain the standard or review an existing service provider." *Steve Ingall, Head of Consultancy, iCore Ltd*

"An outstanding book from the world's foremost authority on the ISO 20000 Standard. As a companion to applying the Standard, this guide is a must for Service Providers." *Sharon Taylor, President, Aspect Group Inc.*

"Standards are the moulds for shaping an industry as it matures. The ISO/IEC 20000 series has played a pivotal role in the growth of formal IT Management approaches, and this new standard will ensure that it continues to do so. This introduction goes far beyond a summary of the standard, and provides valuable insights to the intent, content and practical use of the series." *David Cannon, FSM: Chairman, itSMF International*

About the Authors

Jenny Dugmore works for Service Matters. Jenny has a background in both consultancy and operational line management. She is chair of the ISO group responsible for 20000 series and is co-editor for the new ISO Guidance on the combined implementation of ISO/IEC 20000 and ISO/IEC 27001. She is chair of the ISO committee investigating joint ISO and OGC publications. She is involved in certification schemes and examination boards for ISO/IEC 20000. She is the UK Accreditation Service technical expert on service management. Jenny was winner of the itSMF-UK Lifetime achievement award in 2005.

Shirley Lacy works for ConnectSphere and specializes in the application of service management best practices to deliver value from IT investments. Shirley is highly regarded within the industry and is an authority on service management practices. Shirley is a co-author of the OGC's ITIL Service Transition publication and project mentor for the ITIL update. Shirley has significant experience of helping organizations to adopt ITIL practices and to achieve ISO/IEC 20000 certification. She holds the ITIL Expert certificate and is an accredited trainer for ITIL and ISO/IEC 20000. Shirley is the UK representative on the ISO groups that develop IT service management process and capability assessment standards.

BSI order ref: BIP 0125

BSI Group Headquarters
389 Chiswick High Road
London W4 4AL

www.bsigroup.com

The British Standards Institution
is incorporated by Royal Charter

ISBN 978-0-580-72846-4