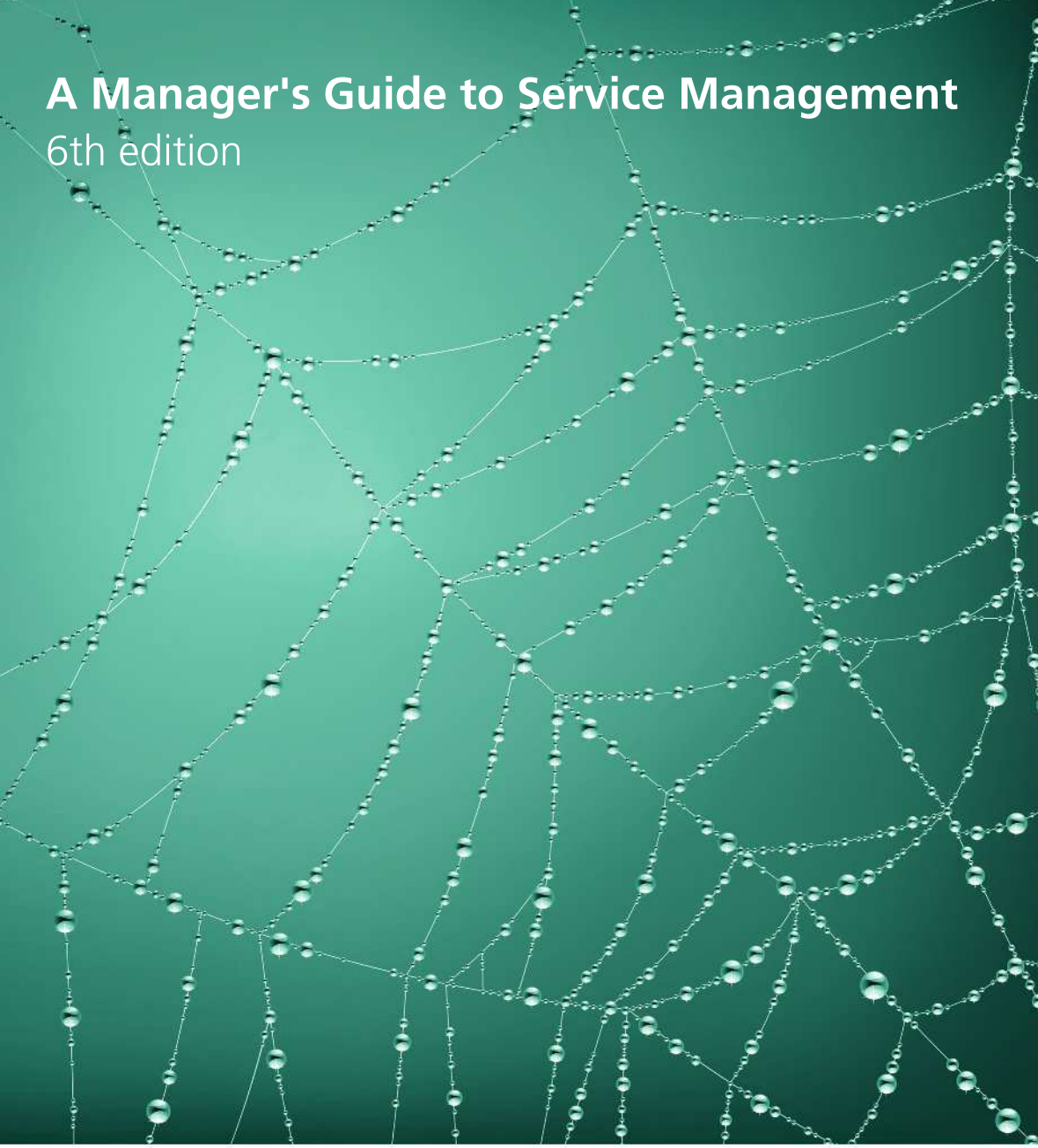

A Manager's Guide to Service Management

6th edition

Jenny Dugmore and Shirley Lacy

BSI

A Manager's Guide to Service Management

A Manager's Guide to Service Management

Jenny Dugmore

Shirley Lacy

First published in the UK in 1995 by BSI, 389 Chiswick High Road, London W4 4AL

Second edition published in 1998
Third edition published in 2003
Fourth edition (with updates) published in 2004
Fifth edition published in 2006
Sixth edition published in 2011

Typeset in Great Britain by Letterpart Limited, 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 72845 7

Contents

Foreword

This guide has been developed to give unbiased advice on the management of services. It is intended for managers who are new to providing customer and supporting services or who are faced with major change to their existing services and support arrangements. It will be of interest to anyone involved in the provision or management of services.

This guide can be used as a manager's guide to service management, including the hybrid use of ITIL®[1], COBIT®[2] and the ISO/IEC 20000 series.

ITIL is a widely adopted approach for service management best practices, based on practical industry experience. It covers identifying, planning, designing, delivering and supporting services to the business and customers.

COBIT is also widely used and is a business-oriented framework for the governance and management of information and IT.

ISO/IEC 20000 was the first series of international standards on IT service management. The core of the series is ISO/IEC 20000-1, which specifies requirements for establishing, operating and improving a service management system (SMS).

This guide is based on the knowledge and experience gained by experts working in the field. It takes the form of explanations, guidance and recommendations. It should not be quoted as if it were a specification or code of practice.

Even though this guide can be used as a stand-alone publication most readers will find it useful to extend their reading to include other publications as well. The reader's attention is drawn to Appendix G, Bibliography and other sources of information, which lists other publications and provides useful addresses, etc.

This guide covers the 'why and what' of service management, touching only briefly on 'who and how'. Details on 'who and how' can be obtained from documents listed in Appendix G.

---

1 ITIL® is a Registered Trade Mark of the Cabinet Office.

2 COBIT® is a Registered Trade Mark of the Information Systems Audit and Control Association and the IT Governance Institute.

While every care has been taken in developing and compiling this guide the contributing organizations accept no liability for any loss or damage caused arising directly or indirectly, in connection with reliance on its content except to the extent that such liability may not be excluded in law.

The guide assumes that the execution of its recommendations is entrusted to appropriately qualified and experienced people.

Preface to the sixth edition

This publication is to help service managers who are responsible for managing the end-to-end life cycle of IT services. Service managers need to focus on creating value and managing change whilst coping with uncertainty and risk. For effective governance of IT they need to focus on key management activities and have the right level of involvement with the business and its customers. Both COBIT and ITIL provide guidance for service managers.

This sixth edition was written following the publication of ISO/IEC 20000-1:2011. It reflects the differences between the 2011 and the 2005 editions of the standard. It also reflects other major developments in service management, including enhancements made to ITIL and COBIT.

Since the fifth edition of this book was published in 2006 ITIL has been updated to focus on creating value and managing change whilst coping with uncertainty and risk. ITIL best practices are structured around a service life cycle and they recognize the importance of governance of IT, globalization, sustainability and different sourcing strategies. COBIT has also been undated to help organizations to bridge the gap between control requirements, technical issues and business risks. Adopting COBIT and ITIL can enable organizations to comply with regulatory requirements.

Acknowledgements

This book has been written with the input and assistance of people involved in the practical aspects of delivering services across all sectors and those actively involved in the development of best practice service management. We would like to thank them for sharing their views and providing constructive criticism and practical experience.

We would also like to thank those who reviewed this sixth edition:

Michelle Hales
Kim Hamilton
Roger Southgate
Anthony T Orr

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

Introduction

Why do we need this guide?

Organizations continue to require increasingly advanced services, at minimum cost, to meet business needs.

With significant change, service providers can struggle to deliver the required service. Working reactively, they spend too little time planning, training, reviewing, investigating and working with customers. The result is a failure to adopt proactive working practices. In addition, processes performed differently cause frustration and mistakes.

Customers are looking for better quality, lower costs, greater flexibility and faster response to their requirements. This means that effective service management is increasingly recognized as fundamental to success. Service management has also increased in prominence in recent years due to the recognition of the need for governance of IT, as a part of corporate governance. Compliance with regulatory and legal requirements, such as the Sarbanes–Oxley Act is part of the reason for this increased prominence. Consistent best practice service management provides the underpinning controls, information and audit trails for governance.

This guide can help service providers to understand standards such as the ISO/IEC 20000 series and how they fit with best practices such as ITIL and COBIT. It will also help people to understand the rules of assessments, audits and certification schemes. It provides a common basis for service management and continual improvement using the ISO/IEC 20000 series, ITIL and COBIT.

An integrated service management system (SMS), including service management processes provides control, greater efficiency and identifies opportunities for improvement. An effective SMS includes effective service management, but what is effective service management?

Effective service management requires service provider staff to be well organized and coordinated.

The variety of terms used for the same process, functional groups and job titles can make service management confusing to the new manager. Failure to understand the terminology can be a barrier to establishing an effective service management capability and SMS.

Appropriate automation and tools also ensure that the processes are effective and efficient. Conversely, poorly managed tool selection or implementation can cause additional overheads and increased rework and frustration.

This guide is aimed at managers and staff responsible for implementing, maintaining, improving, assessing or procuring services. It enables readers to develop a practical understanding of best practices, the benefits and possible problems of service delivery using an SMS.

This guide can also help an organization make appropriate decisions on tool selection, by outlining the processes and activities that are used in best practice service management.

This guide will be particularly useful to:

- managers seeking a broad-based introduction to best practices and standards for service management;
- organizations that must meet governance, regulatory and legal requirements;
- managers who need to make or adapt to major changes;
- staff who want an awareness of the management of services, for example people about to start a training course;
- owners of certification schemes for management system standards, such as ISO/IEC 20000-1 (referred to as Part 1);
- users of COBIT who need to understand how service management supports the governance of IT;
- users of COBIT for an assessment of their service management capability based on Part 1 to support improvement;
- owners of service management qualification schemes for persons;
- customers who use services that can benefit from improved service management;
- procurement departments insourcing or outsourcing services;
- people sponsoring, managing or working on projects that deliver IT-enabled services, for example project managers, business analysts;
- assessors who are to review or audit an SMS or service.

Background to this guide

The individual components of an SMS all offer opportunities for improved service management and services. However, coordinated implementation of an SMS offers much greater benefits. This can be staged or phased, although a long delay in implementing a component can undermine those that have already been implemented.

Service management best practices are unchanged by the organizational form adopted, as described in Chapter 5.

Service providers should adopt common terminology within their own organization. This is the basis for a more consistent approach to service management and reduces the necessity to 'reinvent the wheel'.

The role of management in ensuring best practices are adopted and sustained is fundamental for any service provider. However good a set of best practices is, poor implementation and inadequate leadership can result in the practices failing. Initial adoption will not occur correctly without management backing, nor will the quality of the service management processes be sustained without the continued commitment of management.

Managers should also judge the appropriate level of documentation required to sustain service management. A balance should be struck between too little (which risks inconsistency in approach) and too much (which risks a bureaucratic overhead).

Compliance with Part 1, adopting ITIL guidance or using COBIT should not stifle innovation or the ability to respond to changing circumstances.

Background to the revisions

This edition has been changed to reflect the enhancements to the ISO/IEC 20000 series, ITIL and COBIT since the fifth edition of this guide was published in 2006. The emphasis on the synergy of using a broad base of standards, methods and tools is also new since the previous edition.

Terms and definitions

The terms and definitions used are those given in Part 1, the ITIL and COBIT glossaries. Unless stated otherwise, where there are any differences in terms across the three, Part 1 terms have been used.

All Part 1 terms from the 2011 edition are included in Appendix A, Terms and definitions. Terms commonly used with a special meaning that are not defined in Part 1 are also included. The source of the definition is given. Terms not defined take their normal English language meaning. Sources of the ITIL and COBIT terms are given in Appendix G.

An understanding of specialist terms is advisable for service providers. This understanding means the requirements and recommendations will be interpreted more reliably.

It will also be helpful in understanding the use of the ISO/IEC 20000 series, ITIL and COBIT.

Contents of this guide

This guide outlines an SMS that will fulfil the requirements of Part 1, assessed and implemented using ITIL and COBIT guidance.

This guide also describes the best practices of the individual processes within the scope of service management. It includes hybrid use of the ISO/IEC 20000 series, ITIL and COBIT.

Reference is made to the overarching governance principles. This includes both COBIT and the ISO/IEC 38500 series of standards on corporate governance of IT.

Chapter 1 Business and IT

Introduction

All organizations depend on digital information and information technology (IT) to manage and operate their business. A challenge is to identify what the business wants and how IT can be used to achieve the desired business outcomes. Correctly applying governance principles and service management will enable an organization to achieve its business outcomes and gain other advantages, such as more effective use of information, increasing competitive advantage while managing risk.

This chapter covers the use of IT in the business, the role of governance and service management.

The challenge for business and IT

Organizations need to provide information and IT services effectively and efficiently. Better planning, management and integration of IT within the business are all becoming more important.

The demand for IT services can change dramatically as business needs change. For example, the following business trends influence the use of IT and related services:

- focus on value creation for customers;
- new business models and innovation, often driven by IT;
- growth in trade across the world;
- need for fraud prevention and data privacy;
- using IT to overcome economic challenges and shifts;
- explosion in digital information and related services;
- need for sustainability;
- mergers, acquisitions and divestitures.

Advances in information and communication technologies are also driving significant change. For example:

- move to the cloud;
- the impact of social computing;
- increase in the ability to store and analyse information;
- move to multiple user channels and mobile applications;

- new digital capabilities;
- increase in embedded computing products and devices.

A challenge is to work out what the business wants and how IT can be used to achieve the desired business outcomes. An organization needs to invest in, manage and control its technology and supporting services to achieve these business outcomes.

With closer integration of the business and IT, some organizations are bringing together business-related IT with the disciplines of service management. This means that they have the organizational and technical flexibility to respond to changing business priorities and to deliver against the enterprise/business unit strategy.

The role of corporate governance

The application of corporate governance integrates and institutionalizes good practices for: planning and organizing; acquiring and implementing; delivering and supporting; and monitoring the performance of services and products. Executives, including board directors and other top management, are responsible for corporate governance. In many cases, this is a legal obligation placed on the leadership of an organization. To neglect this responsibility has been shown to be a serious mistake, potentially leading to prosecution and a prison sentence.

The governance framework ensures that an organization's strategies and objectives are fulfilled. Governance principles enable an organization to gain other advantages, e.g. more effective use of information, gaining competitive advantage while minimizing risks.

Governance cannot, and should not, operate in isolation, but must be underpinned by effective control of processes across the business, service providers and other parties.

The responsibility for IT may be delegated to managers within the organization but the directors are accountable for the effective and acceptable use and delivery of IT by their organization.

The term 'governance of IT' relates primarily to the application of corporate governance to the use of IT. This applies to both demand and supply, to achieve required business outcomes (or value) while ensuring risks are managed. For example, business customers and an IT service provider need to work together to plan, design, develop, deploy, operate, manage and apply IT to meet the needs of the business.

The standard for corporate governance of IT, ISO/IEC 38500:2008, is applicable to organizations of all sizes, public and private.

The purpose of the standard is to promote effective, efficient, acceptable and lower risk use of IT in all organizations by:

- assuring stakeholders that, if the standard is followed, they can have confidence in the organization's corporate governance of IT;
- informing and guiding directors in governing the use of IT in their organization;
- providing a basis for objective evaluation of the corporate governance of IT.

ISO/IEC 38500:2008 sets out six principles for good corporate governance of IT that express preferred behaviour to guide decision-making:

1 responsibility;
2 strategy;
3 acquisition;
4 performance;
5 conformance;
6 human behaviour.

The model for corporate governance of IT shown in Figure 1 is based on ISO/IEC 38500.

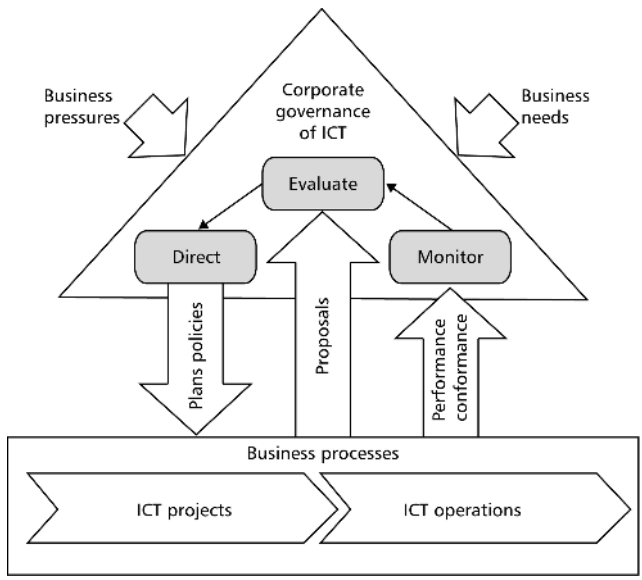

Figure 1 – Model for corporate governance of IT

The model covers three main tasks:

- evaluating the current and future use of IT, including strategies, proposals and supply arrangements, both internal and external;
- direct preparation and implementation of plans and policies to ensure that the use of IT meets business objectives with a clear assignment of responsibility;
- monitoring conformance to policies and performance against plans through appropriate measurement systems, including conformance with obligations.

ISO/IEC 385000 defines Information Technology (IT) as the resources required to acquire, process, store and disseminate information. This includes the composite term 'Information and Communication Technology' (ICT).

Governance and service management

ISO/IEC 20000-1 (Part 1), published in April 2011, defines service management as a 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. Part 1 defines an SMS as a management system to direct and control the service management activities of the service provider.

The top-down approach required for governance of IT is compatible with the top-down approach required for planning, operating and improving an SMS. If correct principles are applied, an SMS is operated within an organization's governance of IT. This in turn is operated within the single corporate governance system of an organization.

As part of governance, the SMS should be linked to the service provider's overall vision, objectives, strategy, policies, processes, resources and information as shown in Figure 2.

The purpose of an SMS is to deliver services that meet business needs and to do this effectively and efficiently. Part of the purpose of an SMS is also to identify and implement improvements to the SMS and services.

This is only realistic if the SMS has relationships to the wider business environment of the service provider's organization, customers, suppliers and partners.

The scope of the SMS will be influenced by these relationships, as described below and in the Introduction to the ISO/IEC 20000 series, IT service management.

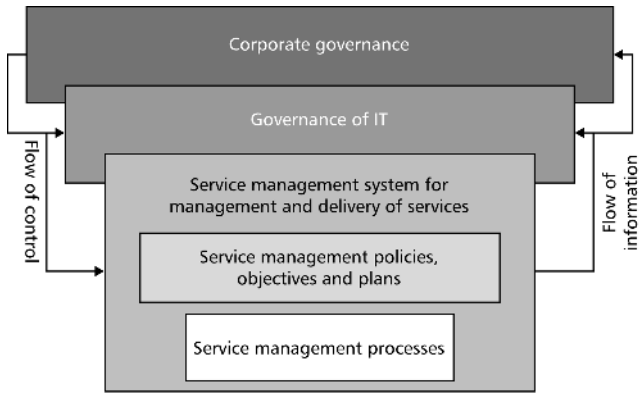

Figure 2 – Corporate governance and the SMS

An example of the relationships between organizations is shown in Figure 3. Within the service provider Organization B, the SMS will need to deliver the business needs of Organization B and comply with the corporate standards, policies and obligations through internal agreements. The scope of the SMS is influenced by agreements between the service provider and the customer (Organization C).

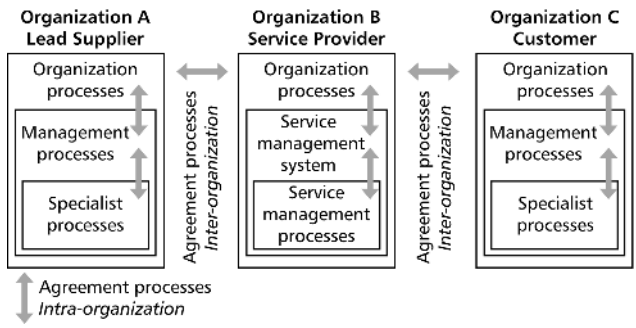

Figure 3 – Example of an SMS and its relationships

Within an agreement, there can be requirements at different levels of the organization, e.g. organization processes, management processes and specialist processes. Similarly, the scope of the SMS will be influenced by agreements between the service provider organization and suppliers, such as Organization A.

Chapter 2 Adapting best practices

Introduction

This chapter covers how other standards and best practices support a manager delivering services to customers.

Several best practice frameworks and international standards can be used in conjunction as part of an organization's overall governance and management framework.

There are many best practices including standards, publically available frameworks and the proprietary knowledge of organizations and individuals. Adapting and adopting the best practices in this publication will assist organizations in implementing service management that supports current and future business objectives and plans. The advantage in using best practices that are publicly available and used worldwide are that:

- they are validated across a range of different organizations;
- they provide a foundation for standardization and common language;
- there is the opportunity for simplification and reuse;
- organizations can benchmark themselves and improve their capability to close any gaps;
- many have associated qualification schemes that help with the professional development of staff.

In addition to ITIL and COBIT examples of standards and best practices that are often used with ISO/IEC 20000 are CMMI, PRINCE 2 and PMI.

Using international standards

Several international standards that are relevant to service management are included in Appendix G. Those that are most relevant are:

- management system standards ISO 9001, ISO/IEC 27000 series;
- ISO/IEC 19770 series on software asset management;
- principle-based standards: ISO/IEC 38500, ISO 31000;
- ISO 9241 series (ergonomics of human–system interaction).

ISO/IEC 20000 and service management

Part 1 provides the basis for assessing whether a service provider has established a successful SMS. It provides the basis for formal certification schemes and other audits.

The requirements in Part 1 are applicable to service providers of all sizes and types, regardless of whether the organization is public or private sector, internal or external. The requirements are independent of the tools used to automate the service management processes and system.

The ISO/IEC 20000 series is therefore not intended to cover:

- governance and governance of IT across an organization;
- detailed guidance on how to do service management;
- how tools are used to automate the service management processes.

ISO/IEC 20000 with other best practices

The ISO/IEC 20000 series can be used with any best practice used to implement an SMS that conforms to the requirements of Part 1.

The Part 1 requirements form a relatively brief set of 'must do's'. Part 1 is the top layer of the pyramid in Figure 4. This is done by assessing whether the processes, procedures and work instructions in the SMS fulfil the requirements in Part 1. This is shown in Figure 4. The assessment will also check that the processes, procedures and work instructions are followed in practice.

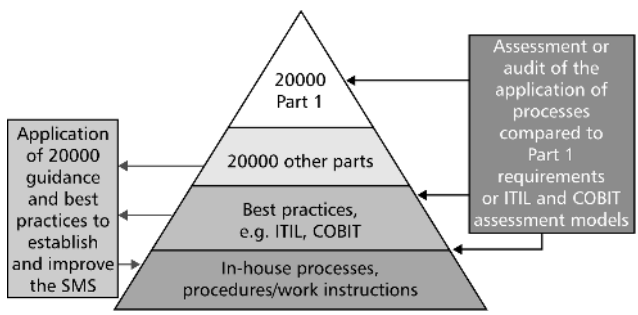

Figure 4 – Using ISO/IEC 20000 and other best practices

The other parts of the ISO/IEC 20000 series help a service provider to plan, establish and improve an SMS. These are shown supporting the top layer, the Part 1 requirements, in Figure 4. These parts of the

ISO/IEC 20000 series also help assessors and auditors to understand the scope, applicability and requirements for Part 1 and an SMS.

Service providers can use other standards and practices to assess, plan, establish, implement, operate, monitor, review, maintain and improve their SMS. The two shown in Figure 4 are ITIL and COBIT.

COBIT and service management

The Control Objectives for Information and related Technology (COBIT) is a governance and control framework for IT management. It was created by the Information Systems Audit and Control Association (ISACA) and the IT Governance Institute (ITGI). COBIT draws from the expertise of the association's members, industry experts, control and security professionals. It provides an objective and practical resource for executive management, business management, IT management and auditors.

COBIT aims to ensure that IT:

- is aligned with the business;
- enables the business and maximizes benefits;
- resources are used responsibly;
- risks are managed appropriately.

COBIT is based on the analysis and harmonization of existing IT standards and good practices and conforms to generally accepted governance principles. It covers five key governance focus areas: strategic alignment, value delivery, resource management, risk management and performance management.

COBIT is primarily aimed at those people in an enterprise that wish to generate value from IT investments, those that provide IT services and those who have a control/risk responsibility. It is driven by business requirements and covers the full range of IT activities. It concentrates on what should be achieved rather than how to achieve effective governance, management and control.

Other COBIT guidance that is useful for service providers includes:

- governance executive briefing and implementation guidance;
- management guidelines;
- IT assurance guide using COBIT;
- how to determine the prioritization of processes to implement;
- COBIT domain and process framework model;
- COBIT maturity models and benchmarks to drive improvement;
- recommendations on authorities and committees;
- responsibilities of business and IT process owners;

- goals and metrics that can be used to align the business and IT goals to measure their achievement and design a management dashboard.

The COBIT framework consists of four domains shown in Figure 5 and 34 processes that define process inputs and outputs, key process activities, process objectives, performance measures and a basic process maturity model. There is also a generic maturity attribute model that is useful for comparing the capability of different processes.

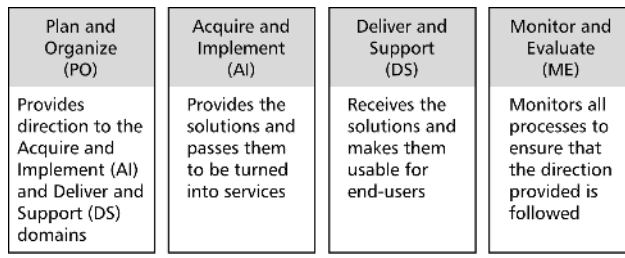

Figure 5 – COBIT domains

Source: COBIT 4.1 © 1996–2011 IT Governance Institute. All rights reserved. Used by permission.

The COBIT guidance supports service providers to achieve the requirements in Part 1, Clause 4. The AI domain generally supports the design and transition of new and changed services and the DS domain generally supports Part 1, Clauses 6, 7.2, 8 and 9.2.

ITIL service management practices

ITIL is a set of consistent and comprehensive documentation of best practice for service management, used by thousands of organizations around the world. The objective of the ITIL framework is to provide services to business customers that are fit for purpose, stable and reliable. ITIL can be adapted and applied to suit the circumstances of a particular organization to achieve the required business outcomes.

ITIL has evolved and changed its breadth and depth as changes in technologies and business practices have changed. One of the drivers for the improvements in ITIL has been the increased sophistication of service management in practical use, driven by ever-increasing demands for an effective and efficient IT-enabled service.

ITIL provides an organization with best practice guidance on how to manage and improve its process to deliver high-quality, cost-effective IT

services. The core guidance consists of five service life-cycle publications that provide best practice guidance for service management. Each core publication covers a stage of the service life cycle:

- **Service Strategy:** key decision making to ensure integration of the business and IT strategies and develop strategies for services that support the business strategy.
- **Service Design:** ensures that each IT service is well designed to meet the customers' desired business outcomes being both fit for purpose and fit for use.
- **Service Transition:** managing and controlling changes to the services and live IT environment, including the transition of new or changed services to meet customer and business expectations.
- **Service Operation:** delivering and supporting operational IT services effectively and efficiently in such a way that they meet business needs, expectations and planned objectives.
- **Continual Service Improvement:** learning from experience and adopting an approach that ensures continual improvement to align the IT services to the changing requirements.

Source: © Crown copyright 2011. Cabinet Office.

The UK Cabinet Office, previously the Office of Government Commerce, retains the rights to all intellectual property, copyright and trademarks relating to ITIL. Its primary role is one of stewardship of the ITIL service management practices framework content and qualifications. There are a range of ITIL examination institutes, qualifications, accreditation bodies and ITIL publishers accessible from the ITIL official website given in Appendix G.

ITIL and ISO/IEC 20000 alignment

An ITIL refresh project led to publication of ITIL V3 in 2007. One of the objectives of the project was to retain and, as appropriate, improve alignment to ISO/IEC 20000-1:2005. The ITIL service life-cycle approach brought a closer alignment to key parts of ISO/IEC 20000.

During the development of the 2011 edition of Part 1, support for closer alignment between ISO/IEC 20000 and ITIL V3 was expressed by the service management community and national bodies. This influenced the requirements for Part 1, e.g. Clause 5. This applies to all changes that have the potential to impact the services or the customer.

There are differences between ITIL and the ISO/IEC 20000 series as they serve different purposes. These are shown in Table 1.

Table 1 – Differences between ISO/IEC 20000 and ITIL

ISO/IEC 20000 series	ITIL
Scope – should be explicitly defined at an early stage for the SMS, as there are limitations on what can be included in the scope of an SMS for certification.	There is flexibility over the scope of the activities to include in ITIL implementation. Fulfilling part of the requirements in Part 1 by using ITIL can bring benefits, even though this might not then be certifiable.
Organizational form – the Part 1 requirements for an SMS apply to all service providers irrespective of organizational form, size, name or types. A service provider can adopt any terms suitable for their circumstances.	ITIL provides guidance on organizational structures, organizational development and organization functions. ITIL includes advice for different types of organization, e.g. internal and external; small, medium, large.
Authorities, roles and responsibilities – must be defined and it must be possible to demonstrate that they are understood.	ITIL provides advice on authorities, roles and responsibilities including committees such as the IT steering committee and change advisory board.
Processes – need to meet the high-level requirements of Part 1. However, Part 1 does not provide any detail on how to design, document and implement a process.	ITIL provides extensive guidance for a range of service management processes that will support a service provider aiming to achieve Part 1 certification.
Automaton and tools – the scope of Part 1 excludes the specification for a product or tool. However, organizations can use Part 1 to help them to develop products or tools that support the operation of an SMS.	ITIL provides recommendations for the use of technology and the basic requirements a service provider will want to consider when choosing service management tools and automating processes.

Using ITIL and ISO/IEC 20000 together

The most common route to achieving the requirements of Part 1 is via use of ITIL best practices. This is such a common route that the ISO/IEC 20000 series is frequently referred to as ‘the ITIL standard’.

Service providers that wish to demonstrate that they have adopted ITIL practices in an effective manner often adopt ISO/IEC 20000. Using the combination of ITIL and ISO/IEC 20000 benefits many organizations.

The ITIL Service Strategy publication covers generic service management principles and processes that are used throughout the ITIL core publications. The ITIL service strategy guidance helps a service provider to scope the SMS, the services and govern processes operated by other parties. There are two strategic areas of focus.

- Align the service provider's strategy with the business strategy, enabling the service provider's organization to achieve its business outcomes (this supports the requirements in Part 1, Clause 4).
- Strategy to plan, establish, implement, operate, monitor, review, maintain and improve the SMS with a service management capability that will deliver services effectively and efficiently (this supports the requirements in Part 1, Clauses 4 to 9).

The ITIL Continual Service Improvement publication covers activities to support continual improvement through the Plan-Do-Check-Act (PDCA) cycle (often referred to as 'Deming') in Part 1, Clause 4.

The ITIL Service Design and Service Transition publications support Part 1, Clause 5.

Details of support for Part 1 by the ITIL books is given in Appendix F, ITIL support for Part 1 requirements.

Practical adaption of best practice

Adapting a common framework of practices that match an organization's needs results in a hybrid approach based on the organization's existing processes as well as adopting industry standards such as Part 1. When adapting a hybrid approach it is useful to understand and map the best practice terms to the terms used in your own organization.

Figure 6 shows an adaption of Part 1 incorporating existing organization processes into the service provider's SMS. The resource management and documentation management processes are organization-wide processes used in the SMS. Other organization-wide processes are included to meet the requirements of Part 1, Clause 4. The continual improvement processes have been adapted.

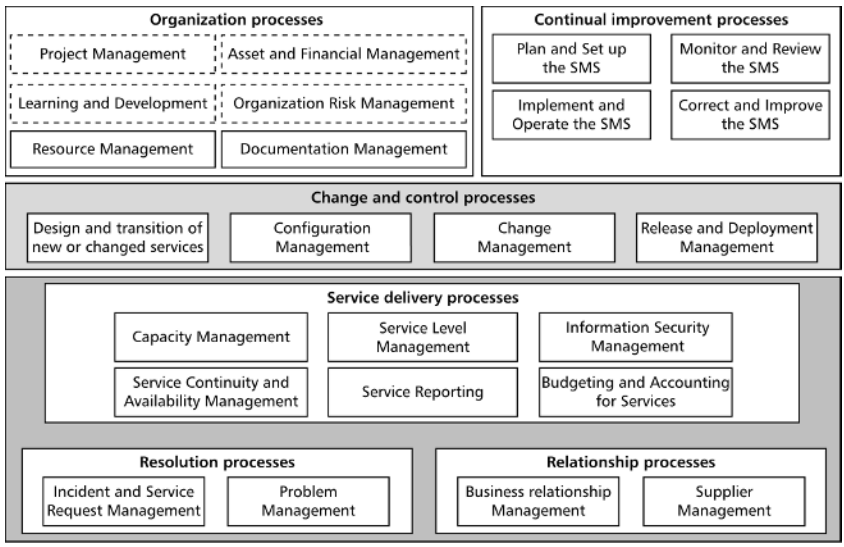

Figure 6 – Example of adapting a process model for the SMS

Chapter 3 Defining services

Introduction

Understanding the requirements of customers and users as well as other stakeholders is an important aspect of service management. A service provider should manage services in a way that demonstrates compliance with a range of service requirements, including any constraints. This chapter describes delivering value from services, the service requirements and approaches to defining the services.

Part 1 defines a service as a means of delivering value for the customer by facilitating results the customer wants to achieve.

A 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.

Delivering value from services

The value of a service for the customer depends on the person that uses the service and what it enables the person to do. The person can be a customer and/or a user of the service. Improvements in service performance contribute to value. For example, a service enables increases in customer productivity and delivers a return on investment. This could be achieved by increasing the transaction rate of invoicing.

Understanding the value created from a service requires practices to measure, monitor and optimize the financial and non-financial returns on investment in the service(s).

Removing constraints also adds value for customers. For example, providing an on-line shop means that a person does not need to travel to the buy goods. Cloud computing services deliver value for the customer by reducing the total cost of utilization, while improving remote access.

Value is also dependent on a customer's preferences. For example, a person who prefers to go to a shop will see no value in shopping on-line. Conversely, someone too busy to go to a shop can find it easier and less time consuming to shop on-line.

Customer preferences are influenced by their perceptions, which in turn are influenced by their:

- experience with a service or similar services/products;
- desires such as being competitive or innovative.

In ITIL, the value of a service is from combining two primary elements:

– **Utility (fitness for purpose)** – this is what the service does. It includes the functionality offered by a product or service to meet a need.
– **Warranty (fitness for use)** – this is how the service is delivered. It is an assurance that the service will be available when needed, with the necessary capacity and reliability in terms of continuity and security.

Service requirements

In the ISO/IEC 20000 series, 'service requirements' is a collective term for the needs of the customer and users of the service and the needs of the service provider. This is unlikely to be one physical document, but there should be a logical grouping of the service requirements as shown below.

These requirements should cover:

- desired results that customers expect from using the service;
- statutory, regulatory, governance requirements and contractual obligations;
- constraints that the service will remove or change;
- use of the services and service components;
- performance and service level requirements;
- planning, establishing, implementing, operating, monitoring, reviewing, maintaining and improving the services;
- constraints from the service provider's business environment including budgets, corporate governance and contractual obligations;
- planning, establishing, implementing, operating, monitoring, reviewing, maintaining and improving the SMS.

A table showing the agreements that are made with the customer is given in Appendix B, Agreements with the customer.

Who contributes to service requirements?

In Part 1, the following types of organizations, groups or people will contribute to service requirements.

- Customers acting as suppliers: groups that rely on the service but who also contribute to the service.

- External organizations: organizations that need to access, use or manage the service provider's information or services.
- Interested parties: individuals or groups having a specific interest in the performance or success of the service provider's activities.
- Internal groups: parts of the service provider's own organization. They can contribute to any stage from design, through to withdrawal of services.
- Lead suppliers: suppliers responsible for managing other suppliers, referred to as subcontracted suppliers.

Service requirements from the customers and interested parties also provide input into the SMS, as described in Chapter 7.

Service portfolio management

In ITIL, the service portfolio is the link between business requirements and the service delivered. It includes the complete set of services that is managed by a service provider and comprises three parts as shown in Figure 7. Business requirements and the service portfolio can be broader than the Part 1 service requirements.

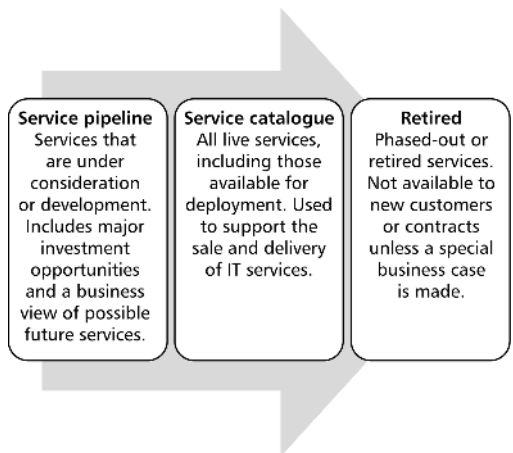

Figure 7 – The three parts of a service portfolio

The service portfolio represents all the resources presently engaged or being released in various stages of the service life cycle across all services.

The ITIL service portfolio management process enables a service provider to provide a strategic view of the business needs and service

requirements of customers. It includes planning the resource requirements across the whole lifecycle. It helps in prioritization and planning of new and changed services. This helps to define the scope of the SMS.

The service portfolio also identifies the customers and users and their specific interests, which is also required for the SMS. It also provides the context for developing Service level agreements (SLAs), contracts, other formal agreements and the service requirements.

A service portfolio covers the life cycle starting with the recognition that the customer's business needs mean a new service is required. Stages in the life cycle and changes of status are:

- recognition of a business need;
- planning and design of the service;
- service development;
- agreement of SLAs, testing and acceptance into operational running;
- inclusion in the service catalogue;
- service removed/retired.

A service that can be improved or changed is managed through the same process and within the framework of the service portfolio.

When a service is removed/retired, the entry is removed from the service catalogue. Documents and records are archived to provide an audit trail of changes, e.g. required for regulatory reasons. The changes to the service catalogue are cascaded through as changes to SLAs, contracts and other document agreements. The impact of a new service can be wide-reaching and result in other changes to the SMS.

The service portfolio provides a framework for Part 1, Clause 5. It also links to the improvements to the SMS and services from Part 1, 4.5.

Defining the service structure and composition

A primary concern of an SMS is delivering the agreed levels of service while managing the demand and supply of services.

ITIL uses a service model to show how the service provider creates the desired utility, warranty and different levels of service for different patterns of business activity. A service model describes the structure of a service (how the configuration items fit together) and the dynamics of the service (activities, flow of resources and interactions). For example, it will outline which personnel will be using the service (user profile), the type of device and equipment and the expected outputs.

The composition of a service and its relationship to its supporting components with related information is important for all stages of the service life cycle. An example is shown in Figure 8. Workloads and service targets are contained within an SLA and supporting agreements, such as Operational level agreements (OLAs). Access to this information will help people within the service provider organization to understand the role of each component within the overall service and its impact on the business.

Some of these aspects are discussed in more detail in Chapter 9.

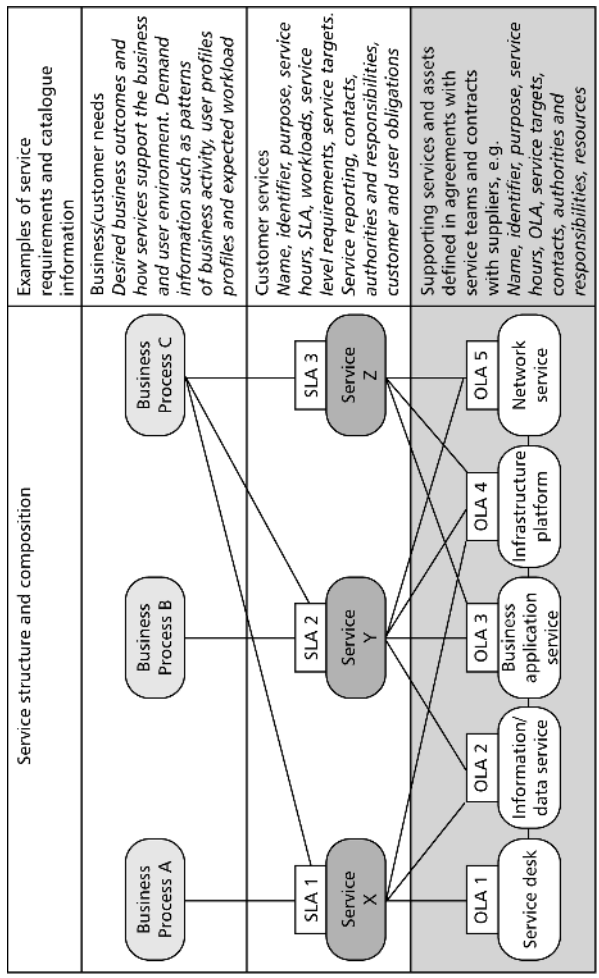

Figure 8 – Example of a service composition and related information

Service provider's requirements

The service provider might be aiming to achieve certification to Part 1 and therefore have specific requirements.

The service provider's requirements will be influenced by the corporate governance requirements of the service provider's organization. Other factors include the requirements of interested parties, in addition to the customers and users discussed above, that interact with the SMS. These requirements affect or are affected by the scope of the SMS. Each party will have service requirements that are influenced by their business environment, the needs of their customers and constraints such as regulations and contractual agreements.

This strategy is an important aspect of the service requirements in Part 1. The service strategy will be translated into responsibilities, requirements, policies and plans for the SMS. An example of the documentation in taking a top-down approach is shown in Figure 9.

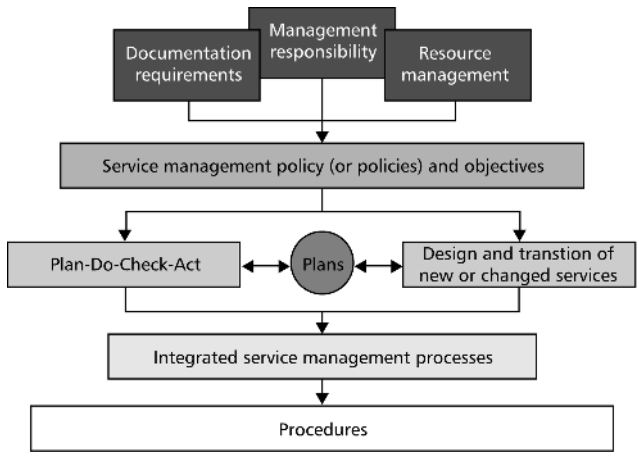

Figure 9 – SMS requirements: a top-down approach

Changes in service requirements

Customers need to be satisfied with and confident in the ability of the service provider to provide the agreed level of service. However, customer expectations can shift and a service provider needs to understand such changes. The ITIL Service Strategy provides advice on how this happens and how a service provider can adapt its services to meet the changing customer environment.

In Part 1 changes to service requirements can be initiated through the business relationship management, service level management and supplier management processes described in Chapters 9 and 10. They can also be initiated through the improvement and change management processes described in Chapters 8 and 12.

Chapter 4 The SMS

What is an SMS?

The normal English language meaning of a system is 'a set of interconnected or interrelated parts forming a complex whole. For example, the transport system' There are also service management systems.

The SMS is a set of interrelated or interacting elements. The SMS establishes policies that provide management direction and objectives as goals for the SMS. The policies and objectives become part of the SMS.

The SMS is therefore a set of integrated components, such as policies, plans, processes, procedures and other underpinning documents and records. The SMS components are necessary for the SMS to function and achieve the service management objectives.

Service management processes are the core of an SMS. Service management is the key difference between an SMS and other management systems, e.g. an ISO 9001 quality management system.

The service management processes are fully integrated. The SMS ensures the processes operate in an effective, efficient and consistent way. This is because the processes are subject to management review, internal audits, other assessments and a continual improvement cycle. This is referred to as the PDCA cycle, described below.

Part 1 authority levels, responsibilities and roles for the SMS are described in Chapter 5.

What is the Plan-Do-Check-Act cycle?

The core of the SMS is the methodology known as Plan-Do-Check-Act (PDCA). The PDCA cycle initially establishes the SMS. The cycle then operates and continually improves the SMS and services. The PDCA improvements apply to all processes in the SMS, including service management.

The four stages of the PDCA repeat in a cycle that is fundamental to continuing control and continual improvement of the SMS and services.

They can be summarized as:

- **Plan:** establishing, documenting and agreeing the SMS. The SMS includes the policies, objectives, plans and processes to fulfil the service requirements and improve services.
- **Do:** implementing and operating the SMS for the design, transition, delivery and improvement of the services.
- **Check:** monitoring, measuring and reviewing the SMS and the services against the policies, objectives, plans and service requirements and reporting the results.
- **Act:** taking actions to continually improve performance of the SMS and the services.

The Part 1 figure illustrating the PDCA cycle is shown as Figure 10. The PDCA cycle is part of the SMS. Because the PDCA acts on the whole SMS it is shown as a cycle encompassing the SMS.

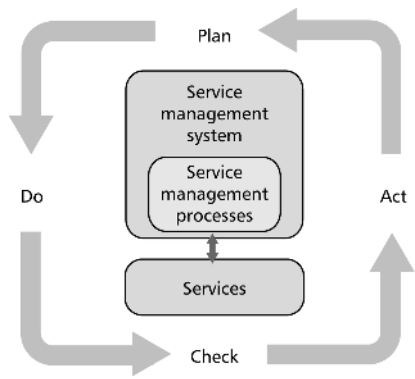

Figure 10 – 'Plan-Do-Check-Act' improvement cycle (from Part 1)

Source: ISO/IEC 20000-1:2011

The more detailed components of an SMS are shown in the Figure 11.

The ITIL Continual Service Improvement (CSI) publication uses the 7-step improvement process that is based on the PDCA cycle:

1 identify the strategy for improvement;
2 define what you will measure;
3 gather the data;
4 process the data;
5 analyse the information and data;
6 present and use the information;
7 implement improvements.

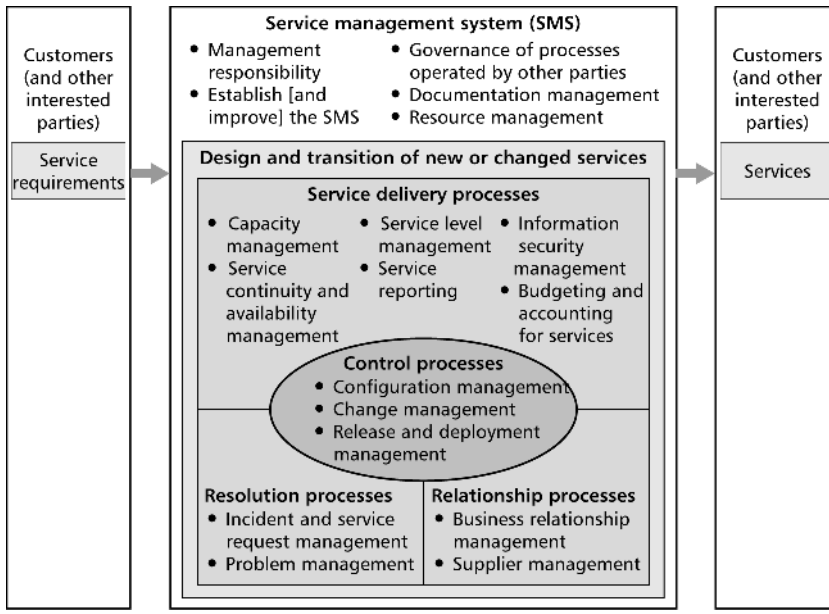

Figure 11 – The components of an SMS (adapted from Part 1)

Source: ISO/IEC 20000-1:2011

ITIL also uses a CSI approach similar to the COBIT approach for continual improvement in the *Implementing and Continually Improving IT Governance* publication. The steps for both approaches are shown in Table 2.

Table 2 – COBIT and ITIL improvement approaches

COBIT Implementing continual improvement	ITIL Continual improvement approach
What are the drivers?	What is the vision?
Where are we now?	Where are we now?
Where do we want to be?	Where do we want to be?
What needs to be done?	
How do we get there?	How do we get there?
Did we get there?	Did we get there?
How do we keep the momentum going?	How do we keep the momentum going?

The COBIT implementation life cycle is a continual improvement approach that provides guidance to enterprises addressing the complexity

and challenges typically encountered during IT governance implementation. There are three interrelated components:

1 the core IT governance continual improvement life cycle;
2 the enablement of change (addressing the behavioural and cultural aspects of the implementation or improvement);
3 the management of the programme.

Defining the scope of the SMS

Rules for defining scope are the same if the service provider and customers are part of the same organization or are separate.

It is important to define the scope of the SMS as the very first stage of establishing the SMS, even if the scope is refined at a later stage. Until the scope is understood and very clear, planning is difficult. The service management objectives will be confused and possibly inappropriate.

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.

The scope should always include the name of the service provider's organization and services.

Other parameters that should be considered for use that will be helpful to avoid ambiguity include:

- location(s) from which the service provider delivers the services;
- the customer and their location(s);
- technology used to provide the services.

Technology owned by another party that is used by the service provider can be named in the scope definition. A service provider can also use other parameters when this is helpful.

Over time the scope can change so it should be reviewed and revised as necessary, e.g. when service requirements change.

Further guidance on scoping and certification is given in Appendix E, Preparing for a Part 1 audit and *Introduction to the ISO/IEC 20000 series, IT Service Management.* Example scope statements are included in ISO/IEC TR 20000-3.

Changing the services

It is rare for an SMS and the services it delivers to remain unchanged for long. Even a small, stable organization can be faced with changes for many reasons. Some of the most significant changes are due to the introduction of new services, the removal of one no longer required or a major change.

In Part 1 the process for the management of a new or changed service is part of service management. There are strong links to project management for the planning/design, building, testing and transition of the service into live operation. There are equally strong links to the other service management processes, in particular the control processes. New and changed services are managed via the release and deployment process.

Criteria in a change management policy define what the service provider will apply the new and changed service process to. These changes are those where the service provider acknowledges there is a higher than normal risk to the service. For example, a change where the potential impact of failure is large or where the change is necessary but difficult.

Changes to the service management policy can also require relatively large changes to be made to the SMS. For example, changes to the service management objectives and plan, to the service catalogue and processes and to the procedures. Changes can impact all other processes in the SMS, e.g. changes to SLAs, service continuity, capacity, incident and supplier management.

Processes operated by other parties

Most service provider's function in a world where there are complex arrangements for the provision of services. Many organizations can be involved, each contributing to the service provider's services.

The contribution by, and governance of, other parties can have a major impact on the scope of a service provider's SMS.

In Part 1 'other parties' are:

- suppliers (and lead suppliers managing subcontracted suppliers);
- customers acting as suppliers;
- internal groups (outside the service provider's direct control).

It is not possible to define the scope of the SMS until the supply chain and the contribution of other organizations is understood.

Defining the scope of the SMS is driven by the nature of the control the service provider has over all groups that contribute to the services. In Part 1 this is 'governance of processes operated by other parties'. Governance is not defined as a special term in Part 1 so it is has the normal English language meaning of 'authority or control and the system of government (as applied to processes)'. This is similar to but not the same as the definition of governance used in COBIT:

> *IT governance is the responsibility of executives and the board of directors, and consists of the leadership, organizational structures and processes that ensure that the enterprise's IT sustains and extends the organization's strategies and objectives.*

Source: COBIT 4.1 © 1996–2011 IT Governance Institute. All rights reserved. Used by permission.

The service provider has the same type and level of control over the processes operated by other parties as they do over the processes the service provider operates itself. Part 1, 4.2 includes:

- 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 Part 1, Clauses 5 to 9;
- determining process performance and compliance with process requirements;
- controlling the planning and prioritizing of process improvements.

For example, the Part 1 requirements for governance can only be achieved if the service provider has control over the design of the processes. This includes the authority to ensure the other party changes the process, when this is needed by the service provider.

In addition, improvements and other changes to the processes must reflect the service provider's priorities. This is the case even if the service provider has no actual involvement in implementing the improvement or change to the process.

If the service provider has governance of processes, the contribution of the other parties is included in the scope of the SMS. When this is the case, only the name of the service provider's organization will be used as a parameter. The name of the other organizations will not be included.

The governance of processes supplements, supplier management and service level management. Suppliers are managed under a process that fulfils the requirements of Part 1, 7.2. Internal groups and customers acting as suppliers are managed with a process that fulfils the requirements of Part 1, 6.1.

The service provider remains accountable for the services or components of services, irrespective of the role played by other parties.

Service management processes

Service management processes are fully integrated parts of the SMS. The model shown in Figures 10 and 11 includes the service management processes within the SMS. These are summarized below and described in more detail in Chapters 9 to 12.

Service delivery processes

The service delivery processes are generally proactive. They are:

- service level management;
- service reporting;
- service continuity and availability management;
- budgeting and accounting for services;
- capacity management;
- information security management.

Relationship processes

The relationship processes are those processes that are most involved in the interface between the service provider and the customer/business. They are:

- business relationship management;
- supplier management.

These two processes span the interface between the service provider and any suppliers, lead suppliers, subcontracted suppliers, internal groups providing part of the service or customers acting as suppliers.

Resolution processes

The two resolution processes are focused on incidents, service requests and problems being resolved or avoided. There are differences between the ISO/IEC 20000 series and other best practices, such as ITIL. In this book they are separated into:

- incident management;
- major incident;
- problem management;
- service request management.

Part 1 treats the resolution processes as two main categories. The first is incident and service request, the second is problem management. Incident management includes major incident management.

Resolution processes are often centred on a front line support group, such as a service desk. However, the resolution processes span organizational boundaries. For example, the process can be operated by first-level and second-level support groups and other parties. This includes suppliers that are part of different organizations.

The management of service requests is also closely linked to incident management, with many parallels between the handling of incidents and service requests. Under Part 1, the service provider may implement incident and service request as a single process, with variants at a detailed level, or as two separate processes.

Control processes

The three control processes are focused on managing changes, releases and configuration items. They reduce risk and prevent interruptions to services and so are fundamental to the longer-term quality and cost-effectiveness of the service.

They are:

- configuration management;
- change management;
- release and deployment management.

Configuration management involves the unique identification, recording and reporting of components, their versions, constituent components and relationships. The term ‘asset management’ is largely synonymous with ‘configuration management’, but is usually used for configuration items with a financial value.

Change management reduces the risk of service or financial loss, fraud, fines, wasted resources, security breaches and damage to the service provider’s reputation. Change management plays an important role in providing an audit trail of events for regulatory reasons.

The release and deployment management process ensures that a set of changes are logically grouped, tested and released. The grouping provides benefits such as economies of scale that reduce the unit cost of making a change.

☑ Benefits

- Improves resource utilization, productivity and value for money.
- Reduces risks, cost and time to market for services and products.
- Improves value for money and service quality.
- Assists in achieving compliance with regulations.
- Service provider is more responsive with services that are business led rather than technology driven.
- Projects plan better balancing of benefits against risks.
- More innovation through technology-enabled change.
- Good understanding of the customer's requirements, concerns and business activities.
- Reliable support for business critical services.
- Resources available when required.
- Greater customer satisfaction with the service.
- Supports the development of a good business relationship.
- Ability to manage suppliers effectively.
- Useful statistics enabling better decision-making.
- More stable work environment.
- Recognition of the value of staff, service and service management.
- Provides support staff with goals and an understanding of their customers' needs.
- Better utilized staff, improved motivation and lower staff turnover.
- Clear career structure and opportunity for career development.

Interfaces and integration

The planning and implementation of the service management processes should take into account the relationships and interfaces between the service management processes. The planning should also take into account interfaces between service management and the rest of the components of the SMS.

The exact details of the relationships will depend on the organization. The interfaces can be direct between two processes and or indirect, when information passes between two processes via an intermediate process.

It is very important for each service provider to understand and optimize the interfaces for their own organization. For example, what information flows to and from a process to policies, other processes and procedures? Other examples are service management objectives, service catalogues,

supplier contracts and service management procedures interacting with the service management processes. The service management processes are aimed at providing the best possible service to meet a customer's business needs within agreed resource levels, i.e. service that is professional, cost-effective and has minimal risk.

The service management processes can be applied with similar benefit to any service delivery operation, including non-IT service providers. There are also many parallels between the SMS and management systems for quality management (ISO 9001) and for information security (ISO/IEC 27001).

Both relationship processes have a strong interface to service level management (SLM). Collectively, supplier management, SLM and business relationship management are closely involved in the management of the supply chain that spans organizational boundaries. The supply chain as a whole is fundamental to the delivery of the service required by the customer. Changes in any one process can affect the other two. For example, a change to a supplier's contract filters through and affects service delivered under an SLA agreed between a service provider and customer. Services provided by suppliers that are incompatible with the service requirements agreed with the customer can be the result of ineffective interfaces between processes.

☒ Possible problems

- Bureaucratic processes requiring a high overhead for service management.
- Too many long documents describing processes and procedures.
- Documents allowed to become out of date.
- Failure to get management commitment.
- Lack of commitment to the process from the responsible staff.
- Lack of training in service management processes.
- Staff expected to adopt service management roles that are contrary to their personalities or technical backgrounds.
- Too little time for feedback and improvement of processes.

Chapter 5 People and the SMS

Introduction

Part 1 describes a number of roles, authorities and responsibilities for an SMS. Many organizations have implemented a successful SMS by incorporating this aspect of Part 1.

The roles of senior management should include resolving barriers to change within the service provider's organization. They should assist in creating a positive view of the SMS and services among customers and users, plus any other parties involved or interested.

Delivering a successful service is heavily dependent on the people selected for the roles involved. The wrong person or a badly trained person can make a process ineffective. Service management roles, responsibilities and competencies should be defined and maintained as job requirements change.

The manager with overall responsibility for the SMS and those responsible for processes in the SMS should be involved in decisions on the design of the SMS. Staff who understand how they contribute are more likely to be motivated and effective.

Process vs. function

While there can be differences in procedures, at a high level processes are a common denominator across service providers. This is the case whatever the size or nature of the organization.

A process can have a variety of names, depending on the service provider's circumstances. Some names are unacceptable for historic reasons, e.g. the name given to a process that was implemented badly can have negative connotations. A single process name can be given to two processes that are very closely integrated, such as service level management and business relationship management.

The differences between a process and a functional group or organizational structure are common for a process such as change management. This can be controlled by a functional group known as 'Change Management'. However, processes such as change management

can be operated by more than one group within the service provider's organization. They can also be operated by both the service provider and other parties, such as suppliers.

In contrast, the group primarily responsible for incident management is not normally known as 'Incident Management'. This process is usually associated very closely with a help desk or service desk.

Often there is a group known as 'Capacity Management', but this group is often only responsible for technical capacity, such as server space. Aspects of capacity management are commonly distributed among other groups. For example, a support group that does capacity management for resources such as number of personnel.

Who is responsible for the SMS?

The senior management in a service provider's hierarchy, referred to in Part 1 as 'top management', has overall authority and responsibility for the SMS. This also contributes to the top management's responsibilities for governance, information security, legal and regulatory requirements. Top management are also commonly referred to by names such as 'Senior Leadership Team'.

Top management should also never lose sight of the continuing accountability for the processes operated, or partly operated, by other parties that are not under their direct control.

Management direction and leadership

An effective SMS is based on the management direction provided by top management's policies and service management objectives.

Once the management direction is available, top management should then delegate to another 'responsible manager' sufficient levels of authority to ensure the activities required for the establishment, operation and improvement of the SMS are actually performed. The role of 'responsible manager' is given a wide variety of names, including service owner, service manager, heads of service, although none of these terms are used in the 2011 edition of Part 1.

In Part 1, a responsible manager role assigns levels of authority and responsibility to other managers for each process and for stages of the process life cycle. These managers are often referred to as 'process owners'. Collectively the top management, responsible manager, service owner(s) and process owners are the management team responsible for the SMS.

A process owner's responsibilities include ensuring each process supports the relevant policy and service management objectives. This spans the SMS design stage through to operation and then improvement. Different people can be given responsibility for design, operation and improvement of the SMS.

The responsible manager also ensures the service requirements are understood and input to the SMS, as described in this chapter as well as Chapters 7 and 8.

A manager responsible for the quality of a process is normally also responsible for effective integration of the process as part of the SMS. It is also necessary to ensure the process is actually followed in practice and, when necessary, changed. This aspect of process integration is fundamental to a successful SMS.

The delegation of authority and responsibilities comes with the obligation to report to top management and for top management to use the information to take a continuing active interest.

Resistance to change can be due to organizational culture and staff or management attitudes. Often this is the result of past events, e.g. failed attempts to adopt best practices. Managing the cause of any barriers requires leadership and clear and consistent policies, including a supportive personnel policy.

Following implementation of an SMS, subsequent improvements and other changes require the same management leadership and involvement.

Service providers that focus solely on implementing and performing service management processes will not obtain the benefits of the PDCA improvement cycle. Nor are they likely to meet IT governance, regulatory or legal requirements. Each phase in the PDCA cycle is equal in importance. Any stage can be a weak link and failure to implement and manage the requirements for each stage will undermine the whole cycle.

Authority levels

One important aspect of an SMS is the identification of the authority levels and responsibilities of the management team. Responsibility for an aspect of the SMS, such as a process, may be combined with operational responsibility for a team of support staff. However, the two types of role are different. A decision on whether to combine the roles as the responsibility of a single individual or to keep them separate is based on local circumstances. Often the drivers are the size of the service provider's organization, the maturity of the SMS and the rate of change that they are managing.

The question of who should be 'top management' is most easily resolved by linking the role to the management with the appropriate levels of authority and responsibility. If someone being considered for 'top management' cannot be given the level of authority and responsibility required to ensure the SMS and services are managed properly, that potential 'top management' is not suitable. Instead, 'top management' has to be found higher up the hierarchy.

Conversely, 'top management' that are so senior that they have many other responsibilities are less likely to give the necessary time and attention to the SMS and services. Tempting though it is to equate 'top management' to the most senior person in the organization, this can be counter productive. The same logic applies to other roles, such as 'responsible manager'.

Service provider's requirements and obligations

Senior management are responsible for ensuring statutory and regulatory requirements and contractual obligations are met by the operation of the SMS. What is required can vary depending on the sector and country in which the service provider operates. Common requirements include protection of confidential personal data and audit trails of changes that can be required as legal evidence, etc. Contractual obligations include both those to the customer under a service contract, and to suppliers, e.g. licences for use of software.

The senior management all contribute towards corporate governance and governance of IT. For example, providing information that shows processes are controlled.

Operational vs. process quality responsibilities

Different people can be allocated responsibility for the day-to-day operation of a process and the quality and improvement of the process. This is especially common in large organizations.

A generic example of the relationship between responsibility for the quality of a process, the operation of the process and organizational structure is shown in Figure 12. Process owners coordinate improvements and functional managers implement the improvements in their group.

Motivation and competence

An effective member or manager of a service management team is a person who has an enthusiasm for customer service. Someone only

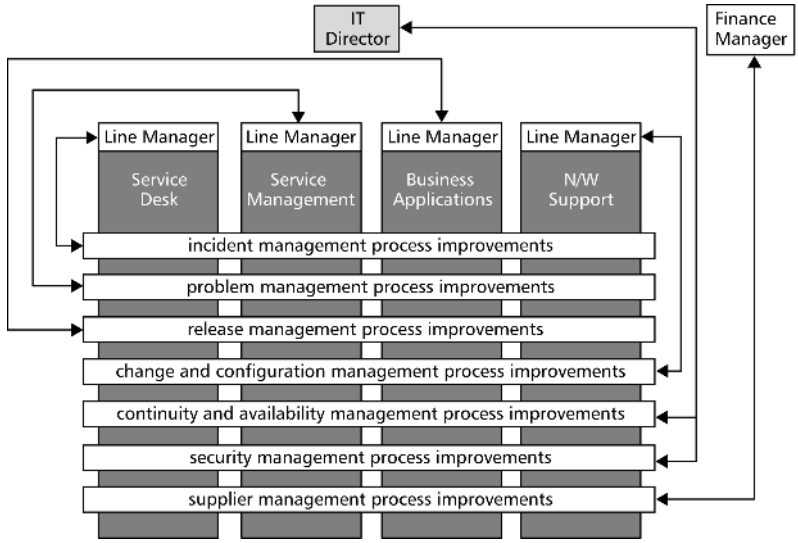

Figure 12 – An example of process vs. function for process improvements

motivated by an interest in technology can be unhappy with a role in service management and an unhappy person is unlikely to be effective. It is important to consider personality when selecting staff.

Introducing variety into the roles of individuals can help motivation, even if there are sufficient people to allow for extensive specialization. This also has the advantage of helping a service provider deal with the peaks and troughs in activity. Mixed responsibilities also reduce dependence on key individuals.

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

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

- short-term or long-term nature of new or changed competencies;
- rate of change in the skills and competencies;
- expected peaks and troughs in the workload and skills mix required, based on current and future technology, service management and service improvement planning;
- availability of suitably competent staff;
- staff turnover rates;

- succession planning;
- training and professional development plans.

Staff require appropriate education, training, skills and experience, all involving good management and personnel practices. Skills usually need to be refreshed as the processes change. A person who is appropriate for planning and initial implementation is not always suitable for an ongoing operation role and vice versa. Temperament, skills and career aspirations all play a part in how well a person does each type of role.

There are a range of training courses and qualifications for service management, covering all three of the 20000 series, ITIL and COBIT.

Stakeholder management

The majority of the management of stakeholders is ensuring communications about changes are suitable for the target audience and provided in a timely manner. A single approach to all stakeholders is unlikely to be effective. Stakeholders can vary widely in why they are interested in the service providers' activities, so communications and other aspects of management should take the different viewpoints into account.

Chapter 6 Where are you now?

Introduction

A service provider's service management capability can be seen as a measure of the reliability, efficiency and effectiveness of service management. At a high capability maturity level there is a consistent approach to service management activities and there is continual improvement. This generally reduces risks and increases quality of service, which in turn increases value to the customers and customer satisfaction.

The first steps

Before any major change, including the implementation of an SMS or major changes to the service, it is essential to understand the current situation or the 'As-Is'. Key features of interest are shown in Table 3.

Table 3 – Key features for 'where are we now'

1	Who are the customers and users, including:
	– business activities and plans including peaks and troughs;
	– demand for service;
	– numbers and location;
	– sector.
2	Service provider's organization:
	– vision and business objectives;
	– organization culture and human behaviour;
	– structure;
	– authority levels;
	– established roles and responsibilities.
3	Status of service portfolio, service catalogue, SLAs, including:
	– range and types of services, required and delivered;
	– actual and target service levels;
	– workloads and workload characteristics;
	– capacity and relationship to performance;
	– service continuity arrangements, actual and required;
	– availability requirements.

4	Relevant statutory and regulatory requirements
5	Constraints:
	– service provider's obligations;
	– supplier contracts;
	– documented agreements with internal groups and customers acting as suppliers.
6	Policy, process and procedures
7	Staff records showing:
	– personal achievements against objectives;
	– skills, qualifications;
	– competence;
	– experience;
	– training plans;
	– staff turnover rates.
8	Reports from:
	– performance against requirements and key performance indicators;
	– reviews;
	– internal and external audits;
	– other assessments.
9	Customer satisfaction measurements
10	Complaints and escalations
11	Service improvement plans
12	Details of any recent failures to implement service management

Audits and other assessments

Audits, assessments and reviews are useful sources of information. For example, an internal audit or assessment following a major incident, invocation of a business or service continuity plans. Relevant information can be obtained from audits under other management systems standards, such as ISO 9001 or ISO/IEC 27001.

Assessments help senior managers to understand areas of weakness, risk and what can be done more efficiently. Comparing the current situation with international standards and best practices is a good starting point for assessing current capability and planning improvement, e.g. using ISO/IEC 20000, COBIT and ITIL. ISO/IEC 15504 also provides useful guidance on performing process assessments.

A capability maturity model can be used by an organization as the framework for benchmarking, internal assessment and planning improvement.

ITIL provides a service management process maturity framework. It is based on an assessment against the five areas of:

1. vision and steering,
2. process,
3. people,
4. technology,
5. culture.

The ITIL model has five maturity levels.

COBIT provides guidance on maturity modelling for management and control over IT processes that is based on a method of evaluating processes from a maturity level of non-existent (0) to optimized (5), as shown in Figure 13.

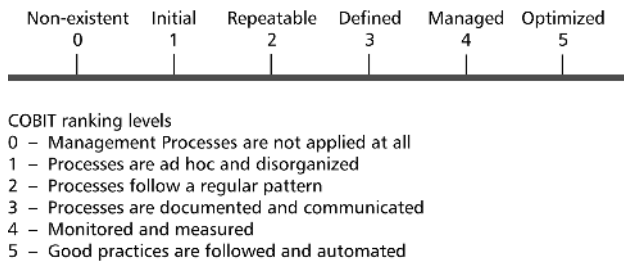

Figure 13 – COBIT maturity levels

Source: COBIT 4.1 © 1996–2011 IT Governance Institute. All rights reserved. Used by permission

COBIT's generic maturity attribute model includes:

- awareness and communications;
- policies, plans and procedures;
- tools and automation;
- skills and expertise;
- responsibility and accountability;
- goal setting and measurement.

This is useful for performing a high-level assessment across a range of processes. An example of assessing two processes is shown in Figure 14.

	Overall	Awareness and Communications	Policies, Plans and Procedures	Tools and Automation	Skills and Expertise	Responsibility and Accountability	Goal setting and Measurement
DS1 Define and manage service levels							
Assessment	2.30	2.20	2.00	1.90	2.15	3.15	2.40
Benchmark	2.15	2.54	2.13	1.88	2.15	2.26	1.94
Difference	0.15	–0.34	–0.13	0.02	0.00	0.89	0.46
DS3 Manage performance and capacity							
Assessment	2.20	2.00	2.20	2.00	2.00	2.00	3.00
Benchmark	2.50	2.82	2.29	2.40	2.53	2.78	2.20
Difference	–0.30	–0.82	–0.09	–0.40	–0.53	–0.78	0.80

Figure 14 – Example of assessment results using COBIT

This is particularly useful when service management is still only at a basic level, for example, well below the level that would fulfil the requirements of Part 1. Typically, this is where only processes such as incident and problem management are established and configuration management is missing or inadequate. Under these circumstances service improvement programmes are ad hoc and usually only attempted following a serious complaint.

This can be combined with the Part 1 requirements to use as the basis of the assessment.

Combining the COBIT assessment levels and Part 1 processes and requirements can be effective for a gap analysis, described below.

Baselining

Baselining can cover the quality of service, service management processes, workloads, customer satisfaction and cost-effectiveness of both the service and service management processes.

It is essential that the relationship between service targets, actual services, service costs and the customer's perception of the service quality is understood. It is also important to understand the effectiveness of the processes as well as the workloads and quality of the service, as all these are strongly linked.

Baselining can include tracking changes in service quality over time (e.g. has the service really got worse, or has it really got more expensive?). Also, if the service quality has changed, what else has changed? For example, service levels are linked to the workloads, support staff headcount and the extent of automation. A rise in support workloads, if not planned for, will have an impact on the service levels within weeks or even days. Service levels might be sustained for a short time by the staff

reacting by working much harder. Sooner or later customers will notice degradation in the service, even if they are unaware of the cause.

It is advisable to baseline before and after major changes. The effectiveness of the change can then be judged compared to the status quo before the change was made. Similarly, the cost-benefit of the change can be measured as well as the impact on the customer's perception of the service. Baselining that involves comparison with other organizations is referred to as benchmarking, as described below.

Benchmarking or gap analysis

After gathering as much relevant information as possible the actuals should be compared to a view of what is required. This is often referred to as benchmarking or gap analysis.

Benchmarking is typically a comparison of the service provider's measurements and observations to the equivalents for other organizations. This is best done at the level of components of the SMS, using the most important features. Attempting to compare every single measurement or observation to an industry norm will not normally be cost-effective as the volumes of comparisons can be huge but the benefits are mainly from broad-based results.

Benchmarking, such as the comparison of service quality, can be limited by the need to make a comparison between organizations and services that are either the same or very similar.

It is essential that the differences between a benchmarking group and the service being benchmarked is understood and quantified if the comparison is to provide useful information. Inappropriate comparisons in benchmarking can be seriously misleading.

If a service provider does not have easy access to industry norms comparison can still be usefully done across different units within an organization. This is particularly the case for large, widespread organizations. Changes over time are also useful.

Part 1 is also effective as a benchmark because it applies equally to all different types and sizes of service provider.

Benchmarking often reveals quick-win opportunities that are easy and low cost to implement, providing substantial benefits in process effectiveness, cost reduction or staff synergy.

Many organizations use benchmarking successfully and find that the costs of benchmarking are repaid through the benefits realized from acting on the information provided.

The benchmark can therefore be made against one or more of four types of information:

1. a baseline set of measures for the same system or department over time, as shown in the example in Figure 15;
2. direct comparisons with similar organizations;
3. industry norms provided by an external organization;
4. other systems or departments within the same company.

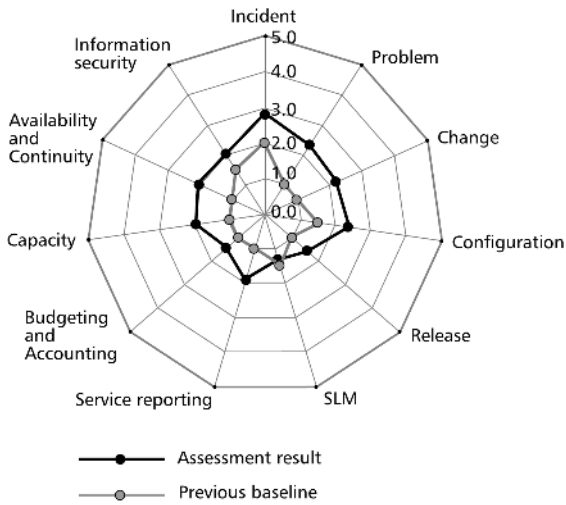

Figure 15 – An example of process capability benchmark

Differences in benchmarking results between comparable organizations are normal, should be understood and can be justifiable. All organizations and service provider infrastructures are unique and most are going through changes. There are also intangible but influential factors, which cannot easily be measured, e.g. growth rate, goodwill, image and culture.

The second and third types involve comparisons with other organizations. Comparison against industry norms provides a common frame of reference. This can be misleading if the comparisons are used without an understanding of the differences that exist across a wide variety of organizations. The differences between organizations can be greater than the similarities. Comparison with a 'typical' result might not be useful as a consequence.

Direct comparisons with other organizations are most effective if there is a sufficiently large group of organizations with similar characteristics. It is

important to understand the size and nature of the business area. Factors to be considered include the geographic distribution and the extent to which the service is used for business or time critical activities.

The culture of the customer's organization also has an influence on the results of benchmarking or gap analysis. Many services are influenced by the extent to which customers will or will not accept restrictions on what they themselves may do with the technology provided. For example, it is difficult to have good security standards with customers who will not keep their passwords secure, or who load unlicensed or untested software on to their computers.

In the fourth type of benchmark, comparison with other groups in the same organization normally allows a detailed examination of the features being compared. This approach means it can be established if the comparison is of 'like with like'. However, it should be noted that some organizations are unusually diverse and have divisions that differ more than other organizations.

Typical benchmarks include measurements that are similar to commonly used service targets or reports. Examples are included in Appendix C, Guidance on SLA and Appendix D, Service management reports. For service levels they can therefore include:

- calls/requests per period, i.e. hour, day, week;
- call/request wait time;
- incident/problem resolution time;
- first-time fix rate;
- remote fix rate;
- incidents/problems solved per person;
- changes made per person;
- units of capacity supported per person;
- customer satisfaction.

They include checks to see if processes or procedures are:

- documented and agreed;
- actually followed;
- managed;
- interfaced to other processes as required;
- subject to continual improvements.

Most benchmarks include some financial measures, such as 'cost per unit'. An assessment of cost-effectiveness is a common reason for benchmarking against other organizations. This is particularly so for service providers that have only limited historic information. These service providers are unable to use service or financial trends to understand whether the service is getting better or worse.

Some customers use benchmarking to decide whether they should change their service provider, insource or outsource.

Benchmarking/gap analysis information is also commonly used for making a business case for establishing or improving an SMS. This information reduces planning time. The plans are also targeted on the use of resources for topics where they will be most effective.

Chapter 7 Plan and set up the SMS

Planning the SMS

The first cycle of the PDCA establishes the basic SMS. Subsequent PDCA cycles identify and implement improvements to the SMS, or extensions to the scope of the SMS. This chapter describes the initial PDCA cycle, based on a scope that has been defined, as described in Chapter 4. It is necessary to decide if there should be a single project or large programme of linked projects.

Operation of, changes to, and continual improvement of, the SMS and services are described in Chapter 8.

Strategy and direction

Planning includes the translation of strategic decisions into an SMS and services. It also includes agreeing service management objectives, service requirements and policies as management direction and understanding how they can be achieved using an SMS.

Implementation of strategic decisions can also require a major change to the service and therefore to the SMS and service management processes. Planning reduces the risk, cost and time required for changes and allows the business to take advantage of the new product or services earlier.

Management direction and documented responsibilities for aspects of planning are essential.

The implementation project will produce outputs, such as new processes. However, it needs to be clear in the business case how the outputs are linked to business outcomes and understood by the key business stakeholders. It is a business case for the business, not for an inward looking project team.

Staged and phased implementation

Planning based on a combination of phased improvements within each of several stages is a common approach. Managed properly it can reduce the risk of the changes. In the ISO/IEC 20000 series, ‘stage’ is used for the

incremental increase in the scope of activities included in the SMS. The first step can be a pilot covering one service or one customer. The next stage is more services, etc. Each subsequent stage increases the scope of the SMS. The service provider adopts improvements so that each stage fulfils all requirements of Part 1.

In the ISO/IEC 20000 series 'phase' is used for improvements over time so that the end of a phase is partial fulfilment of the Part 1 requirements. Advice on phased implementation of an SMS is given in Part 5 and in *Introduction to the ISO/IEC 20000 series, IT Service Management.*

Key points

When planning an SMS it is important to:

- focus on service requirements, based on business concerns, not function or technology;
- link business objectives and related service management objectives;
- clearly define roles and responsibilities including other parties;
- ensure everyone understands and are committed to their roles;
- define the benefits in a way that they can be measured and realized;
- understand how the benefits will be delivered and targets met.

The management team need to ask themselves the following:

- How far should we go?
- Is the cost justified?
- What are the indicators of good performance?
- What are the risks to achieving our objectives?
- How do we compare ourselves to others?

A service provider should also define the objectives that will help to drive effective establishment of the SMS.

Example objectives include:

- to align services with the needs of the business and enable change that maximizes benefits;
- to improve customer satisfaction and the quality of the services;
- to provide more reliable services to support business critical services;
- to reduce the long-term cost of service provision.

Understanding the benefits that the business, the service provider, individuals and stakeholders will achieve from an SMS and the services helps to manage expectations and potential resistance to change. Major changes affect many, if not all, the services and systems used by a business. It is not usually possible to stop 'business as usual' activities.

Planning should cater for events such as:

- business change;
- technology change;
- service improvement;
- infrastructure standardization;
- changes to legislation or regulatory changes, e.g. tax rate changes;
- deregulation or regulation of industries;
- mergers and acquisitions.

☒ Possible problems

- Lack of understanding and commitment can mean the plans are impractical to implement, are low quality and lack credibility.
- The planning is inadequate so that implementation is by stealth.
- Insufficient recognition of the scale of investment in automation results in reliance on manual processes.
- Service providers do not plan suitable phasing.
- If new processes become ends in themselves, the focus on service quality and efficiency is lost.
- Weakness in one process affecting the ability of other processes being able to improve.
- There are no demonstrable improvements because what could be measured, monitored and reported was not understood.

Those responsible for the SMS should be involved from the earliest stage of planning. The staff should assess and plan for the impact on any existing processes as well as existing services. Staff that are involved in this way will buy into the planned changes because they understand the benefits and how they personally will be affected.

A good project or programme management method should be used to ensure that the objective and benefits of service management are achieved within time, cost and quality constraints.

Planning which approach to establishing the SMS is most suitable should take into account the following checklist items.

Strategic perspectives

1. Business need for the new or changed service management processes.
2. Customer's requirements.

3. Management policies.
4. Existing capabilities (e.g. people, processes, information, technology).
5. Risks associated with each type of approach.
6. Size and complexity of the service provider.
7. Timetable and nature of any changes to the service itself.
8. Resources available.
9. Technology or tools available.
10. Other changes taking place.

The impact on different stakeholders

11. Sponsor
12. Customers
13. Users
14. Interested parties/stakeholders
15. Project, development and testing teams.
16. Support
17. Operations
18. Champions
19. Change agents
20. Suppliers, lead suppliers, subcontracted suppliers
21. Internal groups
22. Customers acting as suppliers

Typical costs and resources that should be considered are

23. Resources to implement new and changed processes and systems.
24. Training of service provider staff involved.
25. Software and hardware for databases, systems and tools.
26. Creation and maintenance of accurate management information.
27. Secure storage for hardware, documentation and software libraries.

A plan should also include

28. Quick wins to demonstrate the benefits of the SMS.
29. Starting with something straightforward and using phases.
30. Involving customers, especially those that have been critical of the service.
31. Explaining the differences that will be seen by the customers.
32. Involving suppliers, internal groups and customers acting as suppliers.
33. Explaining what is being done and why to everyone involved or affected.
34. Educating staff to understand the contribution their activities make to the achievements of the service management objectives.

35. An understanding of both the existing services and processes.
36. Setting measurable targets for improvement.
37. Implementation of the new/changed service processes.
38. Defining the requirements and design of the new or changed SMS or services.
39. The interfaces between processes and coordination of interfaces.
40. Identification of risks to the service and how the risks should be managed.
41. People and project responsibilities.
42. Team working, individual competencies, skills and behaviours.
43. New or changed skills of those involved in delivering services.
44. The organization's culture, how to manage barriers that can arise from that culture and the staff's attitude to changes of the type planned.
45. Educating new service managers.
46. The scope and effectiveness of the current automation and an understanding of what can be achieved by the use of new or changed tools.
47. Production or amendment of documentation.
48. Monitoring, measuring and reviewing the SMS and services.

Implementing the SMS

Normal management and project management practices are required for implementing an SMS.

This includes:

- allocation of funds and budgets;
- allocation of roles and responsibilities;
- documenting and maintaining the policies, plans, procedures and definitions for each process or set of processes defined in the plan;
- management of risks to the service;
- managing teams, e.g. recruiting and developing appropriate staff and managing staff continuity;
- managing facilities and budget;
- managing the teams, including service desk and operations;
- reporting progress against the plans;
- coordination of service management processes;
- manage risks and issues.

☑ Benefits

- Improved business and innovation opportunities as the business can take advantage of new services and business change earlier.
- Reduced service outages and risk to the business.
- Increased satisfaction.
- Reduced risk, cost and time required for new products or services.
- Improved business efficiency.
- Greater customer satisfaction.
- Greater reliability of services for business critical activities.
- Improved staff productivity and satisfaction.
- Cost reduction in service delivery or doing more with the same resources.
- Saves time and money.
- The service provider can demonstrate value for money.

Checking the implementation of the SMS

The necessity of monitoring and reviewing the service is usually understood. It is also essential to monitor and review the service management processes, because low-quality service can be caused by ineffective processes.

It is helpful if the SMS includes measures of process performance, i.e. the ability of a process to meet the defined objectives. It is common for there to be key performance indicators (KPIs) for each process to track their performance. Service providers may choose to establish performance metrics based on the service management objectives and their own agreed critical success factors (CSFs).

Monitoring, measuring and analysis should encompass:

- achievement against defined policies, objectives and targets;
- customer satisfaction;
- resource utilization;
- organizational capabilities and competencies;
- trends;
- major nonconformities;
- results of internal audits and reviews;
- financial measures, such as costs and value for money.

☑ Benefits

- Measures of the effectiveness of a process for identification of options for improvement.
- Process control based on the quality of the output of each process.
- Confidence that planned improvements are being implemented.
- Early warning of risks to service changes and improvement initiatives.

Benchmarking, assessments and local reviews by local management can all be used to identify shortfalls in skills, process and technology. There can be a periodic audit against ISO/IEC 20000. The nature and scale of the processes should determine the type of review (or audit) performed against each process.

After a process change, a review or audit should assess processes linked via an interface to the changed process. This is because change in one process can affect others. For example, changes to a release process can influence incident and problem management or change management.

A documented assessment of the shortfalls should be used for planning the next service and process improvements. This is vital to the effectiveness of the PDCA cycle and needs to be demonstrated when service reporting is being audited.

Applying corrections

Some service providers already have high-standard service management. Some already have a service improvement programme established and operating effectively. For these service providers and particularly those with established service improvements establishing an SMS can be relatively straightforward.

For other service providers the scale of changes can be large, involving many interconnected activities spanning an extended period. For these service providers there is the likelihood that the Check stage of the first PDCA cycle will identify changes and other corrections for the SMS. Even if the implementation goes exceptionally well the service provider's circumstances can change during the implementation or review stage.

The first cycle of the PDCA corrects, adjusts or fine-tunes the SMS. This is the same sequence of events as for the later PDCA cycles, when the full established and operational SMS is reviewed, changed or corrected.

Where the service provider has opted for staged increases in SMS scope the later stages are a change to the SMS, as described in Chapter 8.

Changes to the SMS are all done under the control of change management.

Chapter 8 Improving the SMS

Applying PDCA to an established SMS

Changing the SMS can be a result of changes to services. Changes to the SMS can affect the services.

Service providers should recognize the benefits of making the SMS and services more effective and efficient. As a consequence, management reviews and internal audits are fundamental to continual improvement. All those involved need to be aware of their personal contribution. Having a policy on continual improvements and adopting a methodical and coordinated approach helps staff accept the need for changes to their role and to the service management processes. It helps customers accept the implications of the changes to their services.

Major changes to the SMS need to be planned in a way similar to the initial establishment and implementation of an SMS. This was described in Chapter 7. This chapter covers the use of the PDCA cycle to change an established SMS. Changes include new services, new locations and new customers and the impact the change makes on the SMS and service.

☑ Benefits

- Prompt action means the situation is dealt with before it degrades further.
- Continual improvements, when carefully phased, avoid high risks associated with dealing with a crisis.
- Improvements minimize costs of operating a defective SMS.
- Continual improvement of the SMS and services also means that staff are more effective, staff sickness is reduced and staff turnover does not rise.

Following the stages outlined in this guide and in the reference material listed will mean the SMS and services are implemented correctly and are 'fine-tuned' over time. Service providers will avoid the trap of only recognizing the need for improvements when a crisis means corrective action is required urgently.

It is also important for service providers to ensure improvements address causes and not just correct superficial symptoms. For example, if service levels have degraded due to an increase in workloads, recruiting more staff to cope with the increased workload does not address the reason for the workload increase. It is better to balance a short-term need by increasing the number of staff for a limited period. This should be combined with improvements that reduce the workloads.

Quantifying benefits

Before making improvements or other changes, the SMS and service should be baselined. This allows quantified improvements to be compared to the baseline. Actual improvements should be compared to formally agreed objectives to establish if predicted improvements have been obtained. An example of the impact of improved processes on unit costs is given in Figure 16. This includes the costs before and after the improvement.

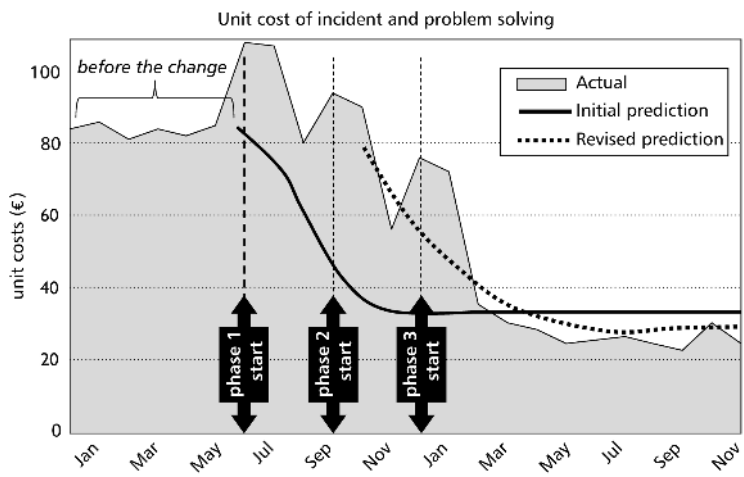

Figure 16 – Example cost savings from an improved SMS

Improved automation, faster problem solving, problem prevention and a change to a service are a few examples of corrective actions that can provide the desired overall correction. It is also easier to justify an increase in headcount if the increased headcount is linked to improvements in the efficiency of service delivery.

Using automation

Automation and tools can help with major improvement programmes by making activities easier and faster (e.g. asset, configuration, change and release management and capacity planning).

The cost of purchasing tools will be less than the total cost of implementation. The following should be budgeted for:

- hardware, accommodation and consumables;
- time for preparing for implementation, data gathering and conversion and testing;
- management time for decisions required throughout the project;
- training of staff to use, administer and support the tools and related processes.

Governance of processes

As described in Chapter 4, service providers are normally dependent on the contribution of other parties for part of the SMS and services. Changes to the SMS need to be communicated to the other parties. For any change to the SMS that directly or indirectly affects other parties, it is common for the contract (with suppliers) or documented agreement with internal groups or customers acting as suppliers to be changed.

Examples include improvement to the configuration management process that must be applied by all parties operating the process. Each party must agree a schedule for the process change that suits the service provider's priorities.

It is inevitable that some other party will be reluctant to comply with the service provider's request for a process change, particularly as this will affect the terms of a legally binding contract. At its most extreme, this means the service provider ceases to have governance of processes operated by another party and those processes or parts of processes cannot be included in the SMS for a Part 1 audit.

The service provider can instead negotiate an agreement with the other party for how this is to be managed to their mutual benefit and so that the certification is not at risk. For example, the other party may make an alternative proposal for the changes to the process.

New or changed services

Special attention must be paid to managing the introduction of new services or changes to services. Every process is potentially involved and

there can be a need for staff recruitment and staff and user training. A well-managed process is a way of avoiding risks and reducing costs.

Proposals for changes to the service, including removal of a service, need to be considered carefully. Factors to consider include the cost, organizational, process, technical and commercial implications of the service change. Planning and implementation should be based on realistic predictions of the budget required. A badly implemented service will not bring the expected benefits and can place the service provider and customers in a worse position than before.

Plans for implementation of new or changed services should include the details given below.

- Budgets and timescales.
- Changes to the nature of the technology supported.
- Infrastructure requirements – hardware, software, network.
- Details of any service closures (e.g. old replaced with new).
- New or changed contracts, SLAs or other service commitments.
- Changes to service management processes, measures and tools.
- Changes to business processes.
- All roles and responsibilities including other parties and customers.
- Skills and training requirements, e.g. technical support staff.
- Manpower and recruitment requirements, including any relocation.
- Overtime hours, e.g. work at night to avoid service disruption.
- Service acceptance criteria.
- User training.
- How quantified benefits/outcomes of the changes will be measured.
- Communication to the relevant parties.

☑ Benefits

- Services are properly designed and successfully implemented.
- Reduction in risk and impact to the existing services.
- Avoidance of services that fail to bring the expected benefits and place the service provider and customers in a worse position than before.
- Better information on the total cost of ownership for each service.
- Actual cost–benefits are reviewed and measured.
- Projects continuing until the new or changed services are fully established.

The service will be at risk unless changes are done under formal change management. Not using formal change management for some changes to the service will also undermine change management itself. A post-implementation review comparing actual benefits/outcomes against those planned is part of change management.

It is also important to have a process by which the new or changed services are accepted by the customer and service provider.

A major service change can mean many smaller changes have to be made at the same time so that more incidents occur, affecting the service levels provided. Also, the testing of changes could influence the availability and response times of the systems.

All service management processes are likely to be affected when a major service change is implemented.

Service management processes

Service delivery

New SLAs, service reports and capacity and contingency are all features that should be considered when planning a major change.

Service level management will need to consider the impact of the changes on the service portfolio, catalogues and SLAs. Changes cascading from revised SLAs to the supplier management process might be needed if the new service requires a different contribution from a supplier.

The established reporting mechanisms can be adequate for use during a major change programme, but this should be checked as part of the planning for the change. Any new or changed reports should be agreed and included in the deliverables from the programme.

Continuity planning includes business impact analysis for major change. Business processes considered to be critical to the survival and success of the service provider will be documented and form a start point for the planning. If a disaster recovery site is available, it can be possible to buy some spare capacity should that be required in the short term.

It is essential that the cost implications of a major change are considered. Budgeting and accounting practices provide a mechanism for predicting and tracking costs. The expected cost of most major changes should have been included in budgets, in advance of the change.

The choice of improvements and other changes can be strongly influenced by the funding available in the current budget year. For example, if the service provider does not have the capital for support

technology, automation is not a short-term option, whatever scale of benefits is predicted. This could be due to inadequate budgeting in the previous year because people did not understand its importance or were unsure of how to produce effective input to budget planning.

With best practice capacity management the capacity of a unit is known. For capacity management the 'unit' can be any or all of hardware, software, people, facilities, etc. The ability to predict 'what if' scenarios assists planning by checking whether there will be sufficient capacity for developing and testing during the major change programme.

The security implications of any changes to the SMS or service need to be considered. If security practices are already in place, then these can be used for the programme. External organizations can be involved in the major change and have access to the SMS, use or manage the service provider's information or services. If this is the case, the planning for the major change will need to take into account the information security controls that the external organization will be required to operate.

Relationship management

By having well-established services and a good relationship with the customer, it is easier to agree short-term amendments to service levels due to major changes. As a minimum, customers will understand what is happening and therefore be more accepting of any disruption or inconvenience during the changes.

Many change programmes involve suppliers. Having commercially sound, working relationships with suppliers as part of service management makes agreeing necessary changes easier. However, it should be noted that there could be a need for changes to the service contract. The change control procedure in the existing contract could be inadequate. Contract renegotiations are usually time-consuming and might be expensive, especially if not started early enough. It is essential to allow for this in the programme budget and timetable.

Resolution processes

Best practice incident management and service request management processes are normally adequate for a change programme. However, additional resources can be required to cope with the increase in workload. It can be necessary to change the level and types of skills and the tools, e.g. new types of service report can be required.

A short-term specialist support group can be a better option than expanding an existing help desk. This approach has the virtue of protecting the normal service. This is a suitable option only if the 'who to

contact when' is unambiguous and the increased support demand is for a short time. A short-term group can be difficult to close as the customers get used to having 'their own' support group.

If support arrangements are unable to cope because there are significant increases in the volume of work, either a delay in the change programme will be required or, under extreme conditions, a major incident declared.

Problem management applies equally well to management of incidents, events and problems from normal services and from major changes. It is even more important to have good problem management during major changes. The existing problem management systems should be used, although customization can be required to accommodate the new requirements and additional specialist staff.

Control processes

Major change programmes can affect all or most systems and services. It is essential to know what exists and what can be affected by the changes, before the changes are introduced.

Configuration management is even more important under these circumstances as the risk of making errors is generally larger than normal. Indeed, many companies find that by preparing for a major programme of changes they have identified many redundant pieces of software as well as being able to track assets more effectively. As a result, they save money by removing redundant assets, capacity, licences and reducing processing time.

Following change management consistently ensures that each request for change is handled in a controlled way. The impact of each change is carefully assessed, costed and prioritized, taking into account all other current work.

Most major changes are best handled by release and deployment management. This groups and tests several changes at the same time, and then implements them as a single release. Good processes and tools for software control and distribution ensure that new versions of software are safely and correctly delivered to their destination, together with any platform upgrades.

Interfaces between processes

Failure to define the interfaces between the components of service management leads to gaps and overlaps, confused staff and reduced effectiveness. This is not only a risk on initial implementation, but the risk

is compounded during subsequent phases. The established interfaces between processes and roles will change during each phase with the introduction of new processes.

One of the major benefits of correct implementation is that roles, responsibilities and interfaces are defined and well understood. Gaps are also identified and can be filled.

Some process interfaces are referred to by Part 1, such as those between change and configuration management. However, the service provider normally has more process interfaces than those referred to in the Part 1 requirements.

All interfaces should be documented, irrespective of whether or not they are explicitly included in Part 1. An input/output table or diagram is a suitable method. This also helps with understanding how the processes interface when documentation is being developed retrospectively. Process integration, required for best practice process management, is dependent on the processes being understood and documented.

Chapter 9 Service delivery processes

Introduction

This group of processes commonly have interfaces that are particularly important to the overall integration of the SMS. Other interfaces exist – for example between service level management and business relationship management and supplier management.

Service level management

Service level management (SLM) identifies and manages agreed levels of service between the service provider and the receiver of the service, i.e. the customer. The service can be provided by organizations that are either internal or external to the service provider's organization.

SLM encourages an understanding of the customer's business drivers, service requirements and definition of service, described in Chapter 3.

SLM includes:

- agreement of the service requirements;
- coordination with other processes and functions, e.g. business relationship management (BRM) and supplier management;
- a catalogue of services written in the customer's business terminology;
- SLAs to support the catalogue;
- reports on service against targets and predicted workloads;
- cost management and cost justification for services;
- fulfilling service requirements and meeting service level targets;
- reviewing the service and agreement of changes to the service, associated costs and workloads;
- input to the PDCA cycle;
- responding to changes to service requirements and business needs.

The customer is primarily concerned that its business can function properly. For example, a payroll department is mainly interested in staff receiving correct payslips on time, not components such as the network.

Service catalogue

As described in Chapter 3, a service catalogue defines the services and targets from the customer's perspective. It can be referenced by other documents in the SMS or refer out to other documents in the SMS, avoiding text or targets being duplicated many times.

Each service provider may structure the catalogue differently, but the catalogue should always set customer expectations. It should be easily accessible and widely available to both customers and support staff, e.g. an intranet site. It should be regularly reviewed and adjusted, e.g. when there are changes to service requirements.

Service level agreements (SLAs)

SLAs are primarily used for details that are unique to a single service or single customer. SLAs can refer to other documents for text common to many SLAs, such as a glossary of terms in a service catalogue. Also, continuity plan(s) and financial details are often referenced from an SLA but not included in detail.

As described in Chapter 3, service requirements are the driver for the SLA contents and structure. The targets are those of the customer, not those of the service provider. The SLAs are negotiated, documented and approved by both the customer and service provider's management. This ensures management backing for the service commitment.

The service provider can opt for either a single SLA with multiple schedules or a series of SLAs. The choice depends on the scale and complexity of the services provided, the geography and the number of customer groups. For example, SLAs at corporate level, business unit or by type of service. An SLA can range from the very simple ('all PC hardware failures will be corrected within x hours') to a complex range of business services.

An overly complex SLA can be the result of distrust of the service provider by the customer. This results in a customer requesting many targets and much supporting detail. A complex SLA can be simplified once the customer trusts the service provider.

As with other documents, the SLA(s) are under the control of change management. It is particularly important that change management considers the impact of changes to SLAs on suppliers' commitments and the overall services. Some changes to SLAs are driven by or cause major changes to the SMS, e.g. new or changed services.

SLA(s) can also be part of a contract when the service provider and customer organizations are legally separate entities. Typically, SLA(s) are a

schedule in service contracts that is overwritten by the body of the contract, because schedules have lower legal precedence. However, only the SLAs are audit evidence for a Part 1 audit.

Supporting information on SLAs is given in Appendix C.

☑ Benefits

- Provides a competitive advantage to commercial business activities.
- Encourages the customers to define their real needs.
- Provides information for sound business decisions.
- The service provider is able to meet the customer's business requirements.
- There is better alignment of actual and required service.
- Service targets, business priorities, impact and costs are acted on.
- Clearly defined customer and service provider responsibilities.
- Avoidance of misunderstandings with customers.
- Clear definition of value for money from service providers.
- The quality of service provided is monitored and easily identified.
- A sound basis for comparisons, ensuring like-for-like assessments.
- A sound basis for input to the PDCA cycle.

Other documented agreements

Other documented agreements in Part 1 underpin SLAs. Typically, these are agreements used to describe delivery of service components. Service components are units of a service that, when combined with other units, provide a complete service, as shown in Chapter 3, Figure 8. These other documented agreements are used to define the contribution of groups within the service provider's own organization. They clarify authorities, responsibilities and roles in the service provider's organization. They are also used for service components delivered by customers acting as suppliers, e.g. specialist business support. In these cases, the documented agreement can be included in a contract between the service provider and customer. An example is shown in Figure 17.

Each significant service component is described and allocated an internal target, e.g. print server availability, network uptime. Many of the targets listed in Appendix C, even if not used in the SLAs, will be relevant to the other formal agreements.

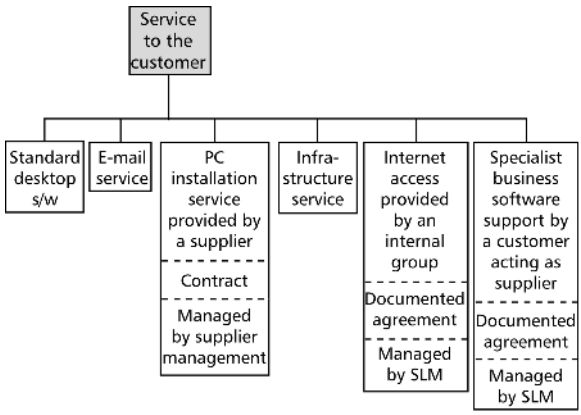

Figure 17 – Other documented agreements

The services are normally invisible to the customer but are essential components of the service. In Part 1 documented agreements are separate from supplier contracts or supplier SLAs, but serve a similar purpose. Documented agreements are not legally binding.

A service provider should not agree an SLA without first understanding the service components. For example, the service provider should not approve a formal target to swapping a customer's PC in four hours if the SLA is for two hours. One of the agreements has to be changed. Which is changed will depend on how important it is to the customer and if it is physically possible to swap in the required time.

☒ Possible problems

- The customer has to learn the service provider's terminology as the service provider does not understand the customer's business.
- SLA(s) are overcomplicated and unmanageable.
- Services are not regularly monitored or reviewed and SLA commitments are based on guesswork.
- Service commitments cannot be delivered with the available resources.
- Service commitments are not supported by a business justification or agreed service requirements and are a 'wish list' or unrealistic aspirations.
- Working practices are not adapted as SLM is introduced or improved.

Service reporting

Scope

Service reporting encompasses all measurable aspects of the service, providing both current and historical analysis. Best practice service reporting is fundamental to SLM, but the best practices and Part 1 requirements apply to all service reporting. Examples include: capacity management, information security and change management. Some aspects of service reporting are similar to document and record management and to the management of information required for reviews, assessments and audits.

There are strong links between service reporting and monitoring, measurement, reviews and other assessments, e.g. the benchmarking described in Chapter 6 and information security management.

Service reports include:

- reactive reports, which show what has happened;
- proactive reports, which give advance warning of significant events;
- reports showing planned activities.

Types of service reports for use in different circumstances include:

- performance against service level targets;
- non-compliance and issues, e.g. against the SLA or security breaches;
- workload characteristics, e.g. volume, resource utilization;
- performance following major events, e.g. major incidents;
- trend information.

☑ Benefits

- Timely, reliable, clear, concise and meaningful information to support decision-making.
- Effective operation of reviews of the SMS and service by providing reliable information on service achievements and workloads handled.
- Proper documentation of tool usage.

Best practice reports

Effective service reports ensure that service providers can plan with confidence and deliver services in a controlled manner, continually improving and making best use of resources. Without reports of

performance against targets and workloads, SLAs with the customer are meaningless. Reports must be available when they are required – a delay can mean the information is no longer of use. This is particularly the case for reports that warn of events or expected difficulties.

It is important that the tools and techniques used are cost-effective. A decision to produce complex reports can require extensive and expensive automation. In this case, the benefits of the information should be balanced against the cost of producing the report. A report should be costed before a decision is made on its final design and production. It can be possible to gain better information for the same cost, or the same information for a reduced cost.

Best practices include:

- a policy that directs service reporting to meet information needs;
- developing and producing reports in a repeatable way;
- ensuring the information provided has fit-for-purpose accuracy;
- checking that the service reports are effective and appropriate.

Service reports should be timely, clear, reliable and concise. They should be appropriate to the recipient's needs. It is essential that reports are objective and relevant to the interests of the target audience.

The requirements for the service reporting process should be agreed and recorded for customers, the service provider's own management and other parties, such as suppliers.

It is usually advisable to have specialist reports with contents matched to specific interest groups, e.g. customers, managers or support specialists. Although each group can have similar interests, a single report should not be used for all readers. It is particularly important for there to be no ambiguity about the algorithms used for the calculation of values and the timetable for production.

Customer management should have reports that state the business issues rather than charts showing trends in urgent problems. They typically include information such as problems with system x, delayed billing for y days, with a cost to the business of z.

The service provider should have, for their own use, reports that help them to monitor and report actual performance against agreed targets, objectives or expectations. These reports should be available at service and service component level. The service provider's reports should also extrapolate service performance and workloads, to assist the planning of continual improvements to the SMS and services. This also requires information on trends and non-compliance or escalations.

Key features of a service provider's reports are information needed to identify preventive actions, not just reporting on the repeated defect

correction. This can involve any aspect of the SMS, e.g. one or more of people, processes or service components used for delivery of the service being unreliable.

A supplier should also report their contribution to the service in a way that directly contributes to the reports for the customer. Ignoring the role of suppliers in delivering the overall service can result in a set of reports that are inconsistent, duplicate each other or have gaps. Where there are lead suppliers and subcontracted suppliers, a lead supplier should report on the whole of the service they provide. This includes services by subcontracted suppliers that they manage for the service provider.

Service reports are required as evidence of the service provider having governance of processes operated by other parties, as described in Chapter 8. Also, the supplier could have been required to implement improvements with a priority determined by the service provider and this should be reported on. These are normally contractual issues, so can take some time to agree.

Examples of service reports are shown in Appendix D. It is important that these examples are not adopted without giving considerable thought to local circumstances and the specific business needs of both the customers and service provider.

Developing and producing service reports

Service reports should be appropriate to the recipient's needs and of sufficient accuracy to be used as a decision support tool. The presentation should aid the understanding of the reports so that they are easy to assimilate, e.g. use of charts.

All reports should be regularly assessed to establish whether they are still useful. A new report should only be agreed if there is a known benefit to be gained from its production.

The following questions should be asked.

- What does the recipient want to know and why?
- Are reports easily understood by the recipient?
- Is the frequency of the report appropriate?
- Are all required supporting data available?
- Who interprets the information?
- Is information collected, analysed and reported with sufficient accuracy for the intended purpose?
- Is information collected to an unnecessary degree of accuracy?
- Does the report imply a greater accuracy than is justified?
- Is the information useful – does it pass a 'so what' test?

- Does each service report include its identity, a clear description, its purpose, intended audience and details of the data source?

☒ Possible problems

- Reporting becomes a routine that adds little value but adds costs.
- The impact of a change to a report on continuity of trend information is not allowed for.
- Tools/techniques unable to measure against agreed targets, usually because an SLA has been badly developed.
- Complex manual intervention to produce reports.
- 'Soft' (non-quantifiable but influencing) factors overlooked.
- Poor presentation targeted at the wrong audience.
- Reports delivered too late to be of use.

Service continuity and availability management

Common features

For most organizations, IT services are essential. Both service continuity and availability management are targeted at delivering services without interruption and within budget. Service continuity is concerned with the speedy restoration of the service following a major disruption. Availability management converts service requirements and any availability targets into a plan for availability and prevents expected and unexpected events that would otherwise result in lost availability.

Some service providers combine these into a single process. If they are implemented as two separate processes, it is essential that the two processes work together.

Both are linked to business plans, service requirements, SLAs and risk management. A business continuity plan, if present, provides a defining structure and major influence upon the service continuity and availability management plans.

Planning should anticipate a wide range of risks. Many risks are due to actions outside the control of the service provider. Examples include denial of service attack, major virus outbreak, terrorist attack or threat of attack, large-scale industrial accident or a natural disaster.

The service provider should have a strategy that defines the approach to meeting obligations. This means the processes are based on an understanding of limits to acceptable risks. Plans for managing

unacceptable risks should be comprehensive. For example, it is of little benefit to have plans for the reinstatement of PCs if access is not possible. Plans should include at least access rights to the services, service response times and availability of services. Access rights are also subject to information security controls.

The service provider should support customers in justifying investment in service continuity arrangements and improved levels of availability. This can be done by providing costs of downtime, business cases, etc.

Both processes rely on there being an understanding of the potential impact of requested changes on the viability of the plans. Even when change management is effective, plans should be reviewed and tests planned and performed. This is also necessary after a major change to the SMS, services or the people responsible for the processes and plans.

Both processes also need to be closely integrated with other processes in the SMS. These include configuration management, information security and the resolution processes. When relevant there should also be an interface to the PDCA cycle.

Plans for both processes should extend into the processes or parts of operated by other parties. Other parties are usually suppliers, when the activities are contractual. Other parties may also be internal groups and customers acting as suppliers.

☑ Benefits

- Services are designed and managed to meet service requirements, including availability targets in SLAs.
- Services are designed to avoid under or over delivery.
- Reduced downtime and maintenance costs.
- Accurate information supports negotiation of service requirements, SLAs, contracts and other formal agreements.

Service continuity management

The service provider should agree and document for each customer and service the acceptable limits to:

- continuous period of lost service;
- periods of degraded service;
- degraded service levels during service recovery.

At least one copy of all service continuity documents should be maintained at a secure remote location, together with any equipment that is necessary for its use.

Service restoration includes the use of:

- criteria to identify when restoration is to be initiated;
- the criteria that dictates prevention or cure during recovery;
- authority levels, approvals and responsibilities for restoration to start and during restoration;
- dependencies between service components;
- actions against each restoration objective;
- roles and responsibilities for each action in the restoration;
- plans and other documents required during restoration;
- backed-up data, documents, software and equipment;
- access to the actual configuration management database (CMDB) or a recent copy of the CMDB.

Testing the plan should jointly involve the customer and service provider. It should be based upon an agreed set of objectives. Testing should be undertaken at a frequency and rigour sufficient to gain assurance that plans are effective and remain so in the face of changes to the SMS and services. Test failures should be documented, reviewed and then input to continual service improvement.

☒ Possible problems

- Difficulty in obtaining experienced staff and/or engendering the correct attitude in staff.
- Difficulty in establishing the service requirements relevant to service continuity and availability.
- Difficulty in translating service requirements into meaningful input into the plan.
- Lack of funds or management commitment to the necessary investment, compounded by the hope that ‘it will never happen’.
- Service continuity plans, contact lists and CMDB are not available.

Availability management

Availability management is a ‘back-office’ process. It involves dealing with how the services are assembled, delivered and supported and is dependent on configuration management data.

Traditionally focus has been on repair time, although in many cases better improvements to the availability will come from prevention and reduction in detection times. Change is the major threat to availability. A temporary freeze on changes for a business critical period can provide the required availability with an acceptable constraint on flexibility.

The customer will consider a service as unavailable whenever they cannot use it. The definition of availability should be based on terms that are meaningful to the customer, if included in an SLA. It is also important that everyone who reads or uses availability measures and targets understands how they are calculated.

Improvement in availability can be from replacing any unreliable service component. Alternatively, this can be by providing fail-safe mechanisms, when alternative facilities are automatically available in the event of a component failure. The latter can often be achieved without the end-user being aware of any apparent loss of service, for example alternative routes between two points in a network.

High availability becomes more complex as processing power is transferred to the customer. It requires vigilance and awareness of both business plans and requirements and internal service provider procedures.

Loss of service should be recorded, investigated and appropriate actions taken. Risks should be identified and preventive action taken.

Budgeting and accounting for services

General principles

Budgeting and accounting for services is fundamental to an effective SMS, service management processes and services, irrespective of whether or not the services are charged for or not.

Many financial policies are based on statutory and regulatory requirements. Consequently, some financial decisions lie beyond the authority level of a service provider's top management. The policies can be set at whole-organization level. However the policy or policies are established they are valid evidence of top management direction. The policies must then be supported by appropriate processes and procedures and the processes must be integrated into the SMS.

Contractual obligations can also need to be taken into account. For example, a customer can include a requirement for financial audit trails in a contract with their service provider. In turn, a service provider may include requirements for financial processes and provision of reports on supplier's activities in the contract with the supplier.

Many decisions on changes and other improvements are influenced by value for money. Budgeting and accounting is therefore important to the SMS because it provides quantified costs of services and service components. The importance of budgeting and accounting is independent of services being charged for or not.

Budgeting and accounting also supports an assessment of the value for money of other parties that contribute to the service provider's service.

Customers are less likely to make unrealistic demands of the service provider when they understand the cost of their demands, even if they do not pay for them directly.

The main areas of expenditure should be identified and broken down into cost units. For example, staffing costs can be broken down into categories such as salary, taxes or training. Each category can be broken down further, for example, training could be broken down into specific courses. Costs should then be budgeted in sufficient detail to enable control and decision-making over the budget period.

The budget figures can become service management targets. As for other targets, the service provider should monitor and report actual costs against the target (i.e. budget) figure. The differences should be reviewed and managed where necessary.

☑ Benefits

- Budgeting and accounting for services assists cost-efficient services and service components, e.g. the unit cost of solving a problem (or the costs of avoiding problems).
- The service provider and the customer can make business decisions on a more sound basis.
- Ensuring that the business provides sufficient funds to run the services it requires through the year.
- Early warning of underuse/overuse of resources.

The detail required

Budgeting and accounting information should be at a sufficient level of detail to allow:

- accounting for suitable cost types;
- apportionment of indirect overhead costs, e.g. flat rate, fixed percentage, or variable element;
- allocation of direct overhead costs;

- information to be appropriate to the customer's organization, e.g. by service for the whole organization, service costs by department or location;
- support for rules on variances against budgets, e.g. size of variance that will be referred to top/senior management;
- impact on SLM or BRM.

Responsible managers should understand how they do the following:

- budgeting and accounting for all service components including:
  - assets;
  - shared resources;
  - overheads;
  - externally supplied services;
  - people;
  - costs such as insurance and licences.
- apportioning indirect costs to services;
- allocating indirect costs to services;
- effective financial control and authorization.

Budgeting

Budgets are usually based on the costs incurred in previous years. Any expected projects, changes to services or workloads are taken into account. It is common for initial budgets to exceed available funds. Budgeting usually then requires planned expenditure to be reduced, delayed until later budget years or funds to be reallocated according to priority.

Financial rules limit the reallocation of funds. Capital expenditure funds for the purchase of assets are not normally interchangeable with revenue expenditure funds for day-to-day costs. For example, funds for one project can be diverted to another. Funds for a support team's salaries can be reassigned to another support team, but diverting project funds to support teams or vice versa is not normally allowed.

What falls into capital and revenue expenditure is partly determined by legislation and within that, by organization-wide rules. Some options are possible, e.g. an organization may switch from using capital for purchase of hardware, to leasing the hardware using revenue expenditure. This flexibility can be useful if capital expenditure is required for a major service improvement programme at the same time that hardware is in need of replacement.

Care should be taken to predict and agree when the costs are expected to occur in the budget year. An unexpected and unexplained variance between budget and actual expenditure can be rapidly escalated and will be time-consuming to explain and justify.

Budgets should be at a level of detail that allows them to be used for service components. It is normally useful to have access to:

- current month figures;
- cumulative 'year to date' figures;
- rest of year forecast figures;
- projected end of year budget figures.

Some service providers also budget for several years ahead as a separate exercise and in support of strategic planning.

Accounting

Many organizations use one-twelfth of the annual budget for each month. Variances against budgets provide a very useful alert for action required to correct the variance. This has a direct link to protecting services throughout the year. If variances are not managed promptly there might be insufficient funds to sustain the service to the end of financial year.

The level of investment in budgeting and accounting processes should be based on the needs of both the customer and supplier for financial detail as defined in the policy.

Accounting should track costs to an agreed level of detail. Accounts should demonstrate over and under-spending/recovery. Accounting should also allow the reader to understand the overall costs of low service levels or loss of service.

Decisions about service provision should be based on cost-effectiveness comparisons. Cost models should be able to demonstrate the costs of service provision.

Optional pricing and charging

If the service provider is external to the customer's organization the customer's budgeted costs are based on charges expected from the service provider. A commercial service provider normally has a profit (or loss) based on the difference between the two. The profit or loss is included in the service provider's accounting and budgeting processes. Internal service providers usually recover costs based on their actual expenditure and on a non-profit-making basis. Some organizations opt for their internal service providers to operate as a profit centre. There are some similarities to the charging by commercial service providers.

Service providers can opt for a charging regime where some services or service components are knowingly under- or over-recovered, e.g. pricing

is used for managing demand. This typically occurs where a service provider has a long-term strategy to reduce costs by completely standardizing the technology used.

Charging policies can be a mixture of different types. For example metered charging, based on the cost of what is used, or flat rate charges for activities that are relatively predictable in scale, scope and complexity.

The impact of a charging policy should be taken into account when predicting workloads. For example, if a pricing policy is that support charges will be the same for all types of PC, old PCs can be retained to save capital expenditure. However, old PCs can be far more expensive to support compared with a new PC.

It is essential that the method, the amount and the payment cycle and process are all understood before the service is taken on. Provision should be made when the budget is being prepared.

Charges are normally raised retrospectively, usually on a monthly basis and in line with the budget cycle.

☒ Possible problems

- If the budgeting and accounting for services becomes too lax, charges are not tracked or recovered, undermining the value of the information.
- If the process is too stringent, it can become an unproductive bureaucratic overhead. This occurs where charging is at a very detailed and complex level or costs are manually tracked and reported. The benefits of charging are outweighed by the cost of tracking, reporting and recovering charges.

Capacity management

Scope

Capacity management ensures that the capacity and performance of the services is appropriate to meet service requirements cost-effectively. This means not too little, not too much, not too soon and not too late. Excess capacity results in unjustifiable and excessive cost. Insufficient capacity leads to performance problems that impact the ability of the customer's business to function effectively.

Service requirements for capacity and performance should reflect the customer's business needs, the service requirements as well as the

predicted effect of changes or improvements to the SMS and services. A key component of capacity management is the prediction of future demand. Capacity planning should ensure that any necessary procurements or upgrades are included in relevant plans and budgets.

Capacity changes can be a reduction in required capacity or performance levels, not an increase. Under these circumstances, capacity management can optimize the impact of reduced demand on capacity and performance, often to achieve cost savings.

Capacity and performance can be used to influence customer behaviour through demand management, e.g. differential charging or specific controls on resource use. It requires a good understanding of business activities and the relationship between capacity, performance, unit costs and human behaviour.

Capacity management involves monitoring, measuring, analysing and reporting on workloads, capacity and performance. Usage and performance levels of the service components should be compared to thresholds. Control mechanisms can be implemented to balance services, balance workloads and change concurrency levels. Capacity management also involves tuning resources and providing changes to capacity based on a prediction of requirements. This is an iterative cycle of operational activities as shown in Figure 18.

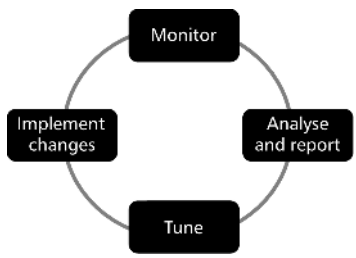

Figure 18 – Capacity management operational activities

Demand management

In ITIL the demand management process aims to achieve a balance between the cost of a service and the value of the business outcomes it supports. The process depends on a good understanding of business activity and how that activity impacts the demand for services.

The ITIL Service Strategy processes (strategy generation, service portfolio management and financial management) define the linkage between business outcomes, the investment required and the required services,

resources and capabilities. It is the demand management process that refines the understanding of how, when and to what level these elements interact.

For example, if a retailer plans to install self-service checkouts at large and small stores, the investment case aims to:

- reduce the checkout queues during peak periods to increase customer satisfaction;
- increase store turnover by 5% for all stores.

To incorporate the self-service checkout into the overall retail service, the designer uses information from demand management and capacity management to model the supply and demand for service. The model showed that the different patterns of business activity in small stores compared with large stores would impact the investment case. Investing in too many self-service checkouts too early in small stores would result in unused self-service checkouts and unnecessary expenditure. The capacity plan was adjusted accordingly.

Capacity planning

Capacity planning should aim to maintain the supply of service against demand while balancing costs against resources needed.

Before a capacity plan is produced, the service provider must understand what capacity is already available and how this matches the service requirements, e.g. demand for service and resource utilization.

A capacity plan, documenting the actual capacity and the performance as well as the expected demand, should be produced. This should be reviewed and if necessary revised at a sensible interval. The actual interval will be determined by the rate of change to service requirements and if there are reports of rapidly degrading performance. It should also be considered before and after major changes, such as the implementation of new or changed services.

Planning should take into account the rate of change in services and service volumes, information in change management reports and customer business. It should include costed options for meeting service requirements and solutions for fulfilling requirements in SLAs.

Part 1 requirements apply to all types of capacity and the plan takes into consideration the following resources:

- technical;
- human;
- information;

- financial.

Technical resources are usually focused on the hardware and software of the infrastructure. This is closely linked to management of the performance of the services against the requirements in the SLAs.

Human resources include actual and predicted headcount and skills compared to service requirements. For example, how many support staff, of what skills levels and types and how will this change?

Information is essential to capacity management. For example, information on: workloads, used and unused capacity, unit costs of capacity and expected changes and how they should dealt with. This information can also be used for 'what if' questions to be evaluated and, if necessary, modelled and calibrated to assist in the process of predicting future capacity needs. Capacity management assesses the cost–benefit of tracking capacity and performance. At a very detailed level the costs can outweigh the benefits.

☑ Benefits

- Reduction in the risks of service failure.
- Cost-effective use of resources.
- Significantly improved planning.
- More informed and economic acquisition of resources.

Financial resources are the funds being available when expected and required. The prediction of capacity and performance costs is improved by effective budgeting and accounting. Capacity plans should be produced in line with the budgeting cycle to ensure funding. Understanding the costs of service components and how these have been influenced in the past allow more reliable projections to be made.

☒ Possible problems

- Unavailable or unreliable business forecasts and information leading to panic buying at higher prices as a capacity issue arises.
- Customer expectations exceed technical capacity.
- Unrealistic and unachievable performance figures from equipment suppliers and manufacturers.
- Too much capacity data for easy analysis, if a monitoring tool is not implemented correctly.

- Purchasing without thinking through the consequences, i.e. knock-on effects.

Information security management

Scope

Information security is the result of a set of controls that identify risks and protect information. Information security management is by its nature an umbrella process that requires awareness of the services and the full environment in which they function.

An information security policy directs how confidentiality, integrity and accessibility of information assets is achieved. It also directs how statutory and regulatory requirements and contractual obligations are met.

In support of policy management, do the following:

- communicate the policy and the importance of conforming to the policy to all interested and affected parties;
- ensure that information security management objectives are established;
- define how information security risks will be managed;
- define criteria for accepting risks that cannot be avoided completely;
- ensure that risk assessments are conducted at planned intervals, with a focus on information security;
- ensure that internal audits are conducted with a focus on information security;
- ensure opportunities for improvement are identified.

Control-based procedures support the information security policy.

The scope includes the implementation, control and maintenance of an information security infrastructure. For example, access by external organizations is subject to controls that reduce the risk of access, use or management of information that should be kept secure.

The ISO/IEC 27000 series is a definitive source of requirements for and guidance on information security management.

General

The risks associated with inadequate information security arise from inadequate controls or controls that are not complied with. The risks are mainly:

- disclosure to unauthorized parties;
- inaccurate, incomplete or lost information;
- uncontrolled and inappropriate changes to information;
- information unavailable or inaccessible when it is required.

These risks are especially high when information can be compromised without the knowledge of the owner or user. For example, systems in which tampering or intrusion cannot be detected.

Information security management depends on accurate knowledge of the potential impact of risks and the costs of problem avoidance. Without them the tendency is either to ignore risks in the hope that they never happen, or expend disproportionate amounts on avoiding risks of minor potential impact.

☑ Benefits

- Security risks are understood at a stage when it is still possible to manage or eliminate them, not after the event of an information security breach.
- No damage to either a service provider's or a customer's credibility.
- Avoids enforcement or legal action.
- It is possible to assign a cost to the actual occurrence of each identified risk and the benefit is the avoidance of that cost, for example:
  - costs of lost production;
  - cost of fraud, fines from regulatory bodies and legal costs;
  - replacement costs of stolen or damaged equipment;
  - compensation payments for unachieved contractual obligations.

Risks are an inevitable feature of service management, but they should be understood and avoided when possible and their mitigation should be cost-effective.

Information security management is concerned with those activities that are required to reduce risks to the point where they are acceptable. It

also then maintains risks at acceptable levels. This includes evaluation of effectiveness of controls and analysis of information security incidents.

Procedures and controls

As a management system standard ISO/IEC 27001 also has a PDCA cycle, referred to in this case as a model. This is shown in Figure 19.

Information security management processes and procedures are control based and support the information security policy and objectives. Each control is linked to a risk, which is described along with how the control is to be operated.

Controls are also reviewed and maintained as information security needs change. The impact of changes on controls should be assessed before changes are implemented.

Information security incidents are recorded as soon as possible, via incident management. Incident management classifies this type of incident as an information security incident.

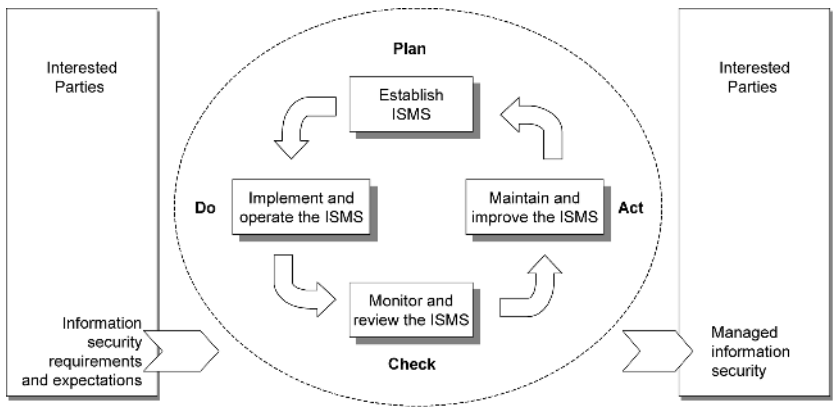

Figure 19 – PDCA model applied to ISMS processes (from ISO/IEC 27001)

Source: ISO/IEC 27001:2005

If the knowledge bases used by the resolution processes show that a method of resolving the incident is known, the resolution is applied and the record is updated. If the incident is a known error with only a workaround possible, this is noted in the record and the workaround is applied. If neither a resolution nor a workaround for a known error is possible, the incident details are passed to problem management for root

cause analysis. Root cause analysis normally leads to identification of how the incident should be resolved. This also results in actual resolution and updating of the record. A new known error is added to the knowledge base.

If the known error cannot be resolved within the expected timescales, a workaround is sought. Problem management then continues to seek a permanent resolution or agrees with the customer that the underlying fault will be left unresolved. For example, if a software package has a security weakness, the resolution may await the release of a new version. The timing of this is not usually under the direct control of the service provider.

In many cases the person reporting the incident will not realize it is a security incident. It is essential that procedures identify security incidents and manage them in a way that recognizes the risks of a security breach and not just a loss of service. It is particularly important to be able to track types, volumes, causes and impacts of security incidents for risk assessment and management of the service as a whole.

This normally requires training so that personnel identify security incidents reliably. Useful information on risk management is provided in the publications listed in Appendix G.

☒ Possible problems

- Security is considered 'someone else's responsibility', i.e. not the responsibility of those who provide, manage or use information.
- Controls are incomplete or inappropriate and influenced by the view that 'it won't happen here'.
- Those who use information or have access for other reasons do not understand the controls, how they are implemented and how they affect their day-to-day activities.
- Controls are not followed and breaches of controls are not identified and acted on.

Cloud computing and security

Cloud service providers offer promises of cost savings, speed to market, increased productivity, easier implementation and better global coverage. However, cloud computing has brought with it some threats. These include deliberate attempts (sometimes successful) to bring down a service by bombarding it with excessive concurrent attempts to access the same web page. The infrastructure has to include resilience to cater for

this. Where resilience is inadequate, the infrastructure has to handle the performance issues, including the loss of access to the service.

Examples of different cloud-provisioning models are:

- private cloud – service managed internally over the intranet or over the internet with a dedicated infrastructure;
- community cloud – cloud infrastructure shared by trusted organizations, managed by an internal or external service provider;
- public cloud – service managed by an external service provider, externally over the internet, usually for multiple customers;
- hybrid cloud – combination of using a public and private cloud.

Each model will bring different threats. Public cloud services might only provide limited security controls. Some organizations need to use a private cloud instead. There can be difficulties in verifying the security and compliance requirements that must be met, e.g. data privacy laws.

Chapter 10 Relationship management

Introduction

The customer facing, strategic process, business relationship management is important to understanding and anticipating changes to the customer's business activities.

The supplier management process ensures that the services provided under contractual arrangements are suitable contributions to the service delivered to the customer. Effective supplier management improves the quality and value for money of the service delivered. The supplier management process also plays a part in ensuring that suppliers are compliant with the requirements for governance of processes, as described in Chapters 3, 4 and 8.

A supply chain is shown in Figure 20.

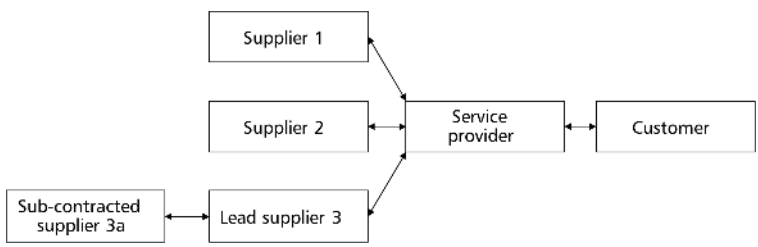

Figure 20 – A basic supply chain (from Part 1)

Source: ISO/IEC 20000-1:2011

Business relationship management

Scope

The scope of business relationship management (BRM) is the relationship between the service provider and the customer, at a strategic level. The

customer may be internal or external to the service provider's organization. There may be one or many customers.

There are close links between BRM and service level management (SLM). Many service providers use a joint service review meeting for both processes, although BRM focuses on more strategic issues than SLM.

BRM ensures that all parties:

- understand the business case and meet business needs;
- understand capabilities and constraints;
- understand responsibilities and obligations;
- understand what customer satisfaction levels are appropriate;
- ensure future business needs are communicated and understood.

An individual is responsible for the relationship, complaints and customer satisfaction. The scope, roles and responsibilities include the identification of stakeholders, contacts and the lines and frequency of communication.

Implementing BRM means that understanding of the customer's requirements, concerns and activities improves. It is beneficial for those involved in BRM to spend time in the customer's own environment.

Where there are several customers the BRM process helps the service provider to understand the differences between them. Effective management of the customer–service provider relationship recognizes and responds to the differences by providing appropriate and agreed flexibility in the services they offer.

BRM is useful for understanding the difference between a business need and a 'business want', particularly if there is no charging to regulate requirements for new or changed services.

☑ Benefits

- Generation of a good relationship, based on an understanding of the customer and the customer's business drivers.
- Improved customer care attitudes and service levels. For the customer it increases its understanding of the role and scope of the service provider.
- Effective BRM means the service provider is aware of business needs with enough notice to be able to react in a timely manner.

BRM and service reviews

The service provider and customer should have an effective communication method and be in regular contact. This includes service review meetings to discuss changes to the business needs, service scope, service requirements, workloads and SLAs. The contract is included if one is present. It is common practice for costs or charges to be considered as part of BRM. The focus of the BRM service reviews is on the customer's business needs, not technology. The reviews use the customer's business terminology and jargon, not that of the service provider.

It is good practice to have a review once a year, as a minimum. Some service providers hold reviews on a much more frequent basis, e.g. before and after major changes.

Options for improvement identified by BRM should also be recorded and input to the continual improvement of the SMS and services.

It is not possible to build a good long-term business relationship without a degree of formality. The normal disciplines of meeting management (e.g. producing an agenda in advance, effective chairing, minutes and action plans produced quickly) should be practised.

Service complaints and customer satisfaction

The cause of satisfaction and dissatisfaction are often outside the direct control of BRM, although it is an important part of the process.

Even with a good relationship, there can be complaints. These are prepared for by a procedure that covers the definition of a 'complaint', who is eligible to make a complaint, how it should be made and who it is made to. The procedure also ensures the complaint is recorded then handled promptly. Escalation should be available to the customer. Complaints are analysed to identify options for improvement.

Customer satisfaction can be measured by several different methods, e.g. regular or ad hoc surveys. Surveys are most effective if they are easy to complete and on what matters to the customer, not the service provider. Those surveyed should be representative of the customer's organization to avoid under or over-representation.

Monitoring levels of satisfaction gives early warning of a gap developing between the services delivered (and defined in the SLA) and the business needs of the organization. Customer satisfaction should be assessed before and after major changes.

Should a customer express serious concerns the service provider should be seen to address those concerns.

Staff should also be kept informed of the results and any action plans. The results should be discussed with the customer, and an action plan agreed. Actions should be reported back to the customer.

☒ Possible problems

- Service review attendance is delegated to junior management without authority for decision-making; discussions are tactical.
- Customer complaints are avoided because it is difficult to complain when the service provider's staff and managers are worried about being blamed.
- A common failing of customer satisfaction analysis is to compare 'apples and pears' e.g. by comparing two organizations that have different cultures, business practices or different levels of funding for services.

Supplier management

A supplier is an organization or part of an organization that is external to the service provider's organization and enters into a contract with the service provider. The supplier's contribution can be for any or all aspects of the service life cycle from service design to improvement and removal of services. The customer need not be aware of the role of suppliers, if the suppliers are well managed.

An individual is responsible for managing each supplier, although the same individual may manage several suppliers. Negotiation skills, financial knowledge and an understanding of at least basic contract law are particularly important for supplier management.

Contracts that describe the service provided are fundamental to supplier management. This includes the scope, service targets, workloads and reporting on performance. The roles, responsibilities, interfaces and integration with the rest of the SMS are also defined.

For any supplier that operates service management processes on behalf of the service provider the contract should define how the service provider retains governance of those processes. For example, control of process design and the priority of process improvements.

How a supplier's performance should be monitored and reviewed is also normally included in a contract.

Lead suppliers are contractually responsible for the management of subcontracted suppliers and are required to demonstrate their capability for this responsibility.

Contracts are reviewed periodically to ensure that they still underpin customer SLAs. Changes are under the control of change management. Suppliers should be notified of changed requirements in a timely manner, especially where there is a complex supply chain. Understanding of changes to responsibilities should be clear and communicated promptly.

Example contract contents are shown below.

Contents of a supplier's contract

In general, any contract that is very much in favour of one party carries a high risk of failing or being terminated early and at short notice. The contract needs to include the following as a minimum.

Scope of the services to be delivered by the supplier

The wording needs to allow the scope to be mapped to the defined scope of the service provider's SMS.

Interfaces and dependencies

This includes the information flowing between processes and how changes to the service provider's processes affect the supplier's processes. It includes interfaces between service management processes operated by the supplier and other parties. It also includes integration of the supplier's activities within the SMS. It should complement the service model.

Requirements to be fulfilled by the supplier

This includes service targets and workload characteristics, in objective and measurable terms, including the details in an SLA, normally as a schedule. A list of contact points within the supplier and service provider organizations is advisable. Although this is not normally part of a contract, a reference may be made to where this information is held.

Contract exceptions and how these will be handled

Most contracts are influenced by what is predicted to happen for the foreseeable future. The unexpected can and does happen and contract exceptions outline the principles of how these will be handled.

Contract change process and procedure

This normally draws a distinction between changes to the body of the contract and to the schedules. The body of the contract normally contains the legally significant clauses, such as the legal system that applies. The schedules are normally used for SLAs, inventories, roles and responsibilities and other features of the supplier's commitment. Changes to the body of the contract are normally handled by people with legal rather than service management backgrounds. Changes to schedules are usually under the control of the change management process, i.e. under the control of the SMS.

Authorities and responsibilities of the service provider and the supplier

This is normally in general terms, i.e. which organization does what and when. Details of individual roles are normally held outside the contract, or possibly in a schedule. The exception is the identity of the people who sign the contract and who are normally those who make a decision on early termination of a contract.

Reporting and other communication to be provided by the supplier

This is information needed by the service provider for effective management of the overall service. The service provider states what is required as evidence of the supplier meeting contractual obligations, including evidence that the service provider has process governance. Effective communications minimize the risk of a dispute. Regular meetings to discuss the reports are beneficial.

Basis for charging

This is variable. Examples include charges per service, per user, per unit of a product being provided.

Dispute management

This is normally legalistic wording. It is usually invoked only if normal review and discussion meetings have failed to resolve the dispute. For example, a persistent failure to meet service targets or refusal to take the service provider's priorities into account when planning improvements. The dispute management procedure aims to avoid a contract being terminated early, but when necessary leads to this.

Early termination and the transfer of services to a different party

A similar process and procedure is required for expected and unexpected termination. Early termination is normally a position of last resort for both parties. However, early termination can be required for other reasons, such as a change in business direction or service requirements

that mean the service and supplier's capabilities are no longer suitable to meet the service requirements.

Supplier management procedures

The service provider follows a procedure that describes roles and relationships between the service provider, suppliers and lead and subcontracted suppliers. This avoids ambiguity regarding who does what.

It is advisable to establish a formal procedure, as part of the contract, to deal with disputes. Attempting to agree a resolution process after a dispute has started adds to the scale of the dispute. Contracts normally include references to which national law applies and in which country legal disputes will be resolved. This can be a relatively complex situation for service providers and suppliers that operate multinationally.

Similarly, a process should also be formally agreed to deal with the expected end of service, early end of the service or transfer of service to another party. There is normally relevant national legislation on issues such as transfer of the service to another supplier that needs to be considered.

☑ Benefits

- A seamless service is delivered to the customer.
- All parties obtain the best value from the relationship.
- A fair basis for support of the service requirements.
- Risk is reduced by defining the role of suppliers, the processes for managing the relationships and agreed SLA targets.
- A good relationship with sufficient flexibility to support long-term service delivery.

From the supplier's viewpoint, good supplier management means that they have an unambiguous role and are judged on an objective and quantified basis. There is a lower risk and fewer problems from the supplier–customer interface, growth in workloads is managed and changes to the contract are amicable. A good supplier management process is not a threat to the suppliers.

☒ Possible problems

- Supplier management is delegated to a manager with technical skills but without supplier management skills.
- There is poor definition of what is sourced from the supplier.
- Supplier's services do not align with or support the overall service to the customer.
- Decisions on suppliers are made without understanding the impact on other parts of the service.
- Inadequate knowledge transfer to the supplier for incident resolution.

Part 1 audits

In a Part 1 audit, the service provider demonstrates conformity to the supplier management process. The supplier is not audited. The scope of the SMS and services requires careful consideration, particularly where the processes cross organizational boundaries.

Chapter 11 Resolution processes

Introduction

The resolution processes are often the first processes implemented. They represent an effective way of keeping the service going. They include incident, major incident, problem and service request management.

Incident management

Incident management restores the service by resolving incidents. When resolution is not immediately possible a method of minimizing the impact of the incident is sought, e.g. a reduced service by disabling a faulty feature. This provides more time for full resolution. Incident management also reacts to incidents that could affect the service but have not yet done so.

If resolution will change a configuration item (CI), this is done via change management. Incident management interfaces to problem management. Problem management identifies the root cause of the incident and its resolution.

Incident management uses information on resolutions, known errors and workarounds developed by problem management. The information is held in a knowledge base used by both processes. Incident management also interfaces to other processes, for information on problems and changes, CIs and the interrelationships between CIs.

Incident management includes the following:

- call reception, recording, priority assignment, classification;
- first-line resolution or referral;
- consideration of security issues;
- incident tracking and life-cycle management;
- incident verification and closure;
- first-line customer liaison;
- escalation.

The volumes and types of incidents are analysed in order to identify areas for improvement, more effective resource usage, cost reduction and improved customer satisfaction. Appendix D lists report types.

Reports of incidents are received by many methods: telephone calls, voicemails, visits, letters, faxes, e-mails. Incidents can be recorded directly by users with access to the system, or by automatic monitoring software. The process converts the information into an incident record.

A single point of contact makes it easier to deal with customer and user issues. A single logical group can be based on distributed staff, following an identical process. The process can cross organizational boundaries. The transfer of information and of control of an incident is important, especially where the process spans several organizational groups or locations. All incidents and any actions need to be logged immediately.

The process is highly visible to users and therefore influences their perception of the service and the service provider. The process is also fundamental to representing the interests of the customers on reactive issues to the rest of the service provider's staff, e.g. BRM.

☑ Benefits

- Timely incident resolution reduces the impact and costs.
- Improved performance against service levels and other targets.
- Improves teamwork, communication and resource management.
- Improves control over other parties involved in the delivery of service.
- Provides important, customer focused, management information.
- Less disruption to customers, users and support staff.

Unpredictability can annoy and create difficulties in managing priorities, so a procedure covers the status of an incident, usually following seven stages:

1 recording;
2 allocation of priority;
3 classification;
4 updating of records;
5 escalation;
6 resolution;
7 closure.

Each stage is necessary, but the sequence is not always as shown. In ITIL there are differences in the names of stages. This list is taken from Part 1.

Resources and activities are allocated according to priority, taking into account the impact of the incident and the urgency with which it should be resolved. Other factors include the availability of resources.

Classification of incidents helps route an incident to the correct group if an incident is not resolved by the group that recorded it. Classification also helps monitoring and reporting.

Classification works most effectively if it is based on a simple hierarchy of short, linked lists. Typical ways of classifying incidents are: category based on suspected cause, priority, affected service and support group.

As the incident progresses the workflow is tracked by using the status of the incident. This is an efficient way of processing and tracking incidents.

Staff should have access to up-to-date information on other incidents, problems, known errors and workarounds. Having this information will make incident resolution better and faster. Information on recent and planned changes, and access to configuration management data showing how service components are interrelated is also useful. Frequently asked questions and checklists to help resolution are an advantage.

The final steps before a record is closed involve updating and completing the record. If any of the information is out of date or incorrect this should be notified to the information owner. The record is closed after it is confirmed that the incident is resolved.

Major incident management

Where possible a major incident follows the same process and procedure as an incident or, if the root cause is obscure, also some aspects of problem management. The major incident process establishes the acceptable deviations from the normal incident management process.

By its nature a major incident is generally high impact, high risk or serious in some other way. It usually requires more resource and management involvement. Major incidents may involve separate aspects of the incident being resolved by different groups, sometimes in different locations, requiring a large overhead for coordination.

The complexities of a major incident means that it needs to be controlled by a single manager, appointed for the duration of the major incident. There may need to be deviations from the normal process and procedure sanctioned by the major incident manager. The major incident manager is responsible for ensuring that each group is aware of the activities of the others and that there is effective communication and escalation.

A major incident review is performed after the service has been returned to normal.

☒ Possible problems

- Service delivery culture is not customer-focused.
- Benefits are not sold to the customers and users.
- Poorly defined service objectives, goals and responsibilities.
- Working practices not being reviewed or changed.
- No agreed customer service levels or priorities to assist workload management.

Problem management

Problem management identifies the root cause and minimizes disruption of the customer's activities by resolving problems in a timely manner and within the agreed target time. The process relies on incident and problem data to identify root causes and preventive action.

This process is largely proactive and interfaces directly to reactive incident management. The interface passes up-to-date information on known errors and corrected problems to incident management.

Problem management includes:

- problem detection and resolution of problems;
- tracking and escalation;
- communicating information;
- resolution that requires a CI to be changed via change management;
- resolution or workaround applied or known error recorded;
- record closure;
- proactive problem prevention;
- review and reporting on the effectiveness of resolution;
- identification of options for improvement of the SMS and service.

It is common for staff performing problem management also to perform incident management and some aspects of service reporting.

The main goal of problem management is the detection of root causes and their eradication or a workaround. This can conflict with the incident management goal of restoring the service as quickly as possible. For example, a network that frequently fails but can be reset quickly. The root cause is left unresolved because this would delay restoration of the service, even if resolving the root cause would prevent recurrence.

☑ Benefits

- Problems are prevented or, if they have occurred, recurrence is prevented.
- If problem resolution targets are at risk or not met, problems are escalated.
- Service levels are improved and costs reduced.
- Customer satisfaction is improved.

Prompt resolution of problems is assisted by reference to similar incidents and problems. It is important to classify problems and record cross-references to previously logged and resolved problems.

When a root cause, a method of resolution or a workaround have been identified the problem is recorded as a known error. Known error information includes current and potentially affected services in addition to the CI considered to be at fault. Known errors are recorded in a knowledge base for use by other service management processes.

A known error is closed only after successful resolution of the root cause, so may be left open indefinitely. For example, the resolution can be considered too expensive or of insufficient benefit. If this is the case, the reasons for this known error being left unresolved should be clearly documented.

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

The status of problems should be tracked through eight stages:

- identification;
- recording;
- allocation of priority;
- classification;
- updating of records, including recording of resources used and actions taken;
- escalation if targets are breached or at risk;
- resolution, if necessary agreed with the customer;
- closure, including accurate completion of the record.

As for incident management, the stages, sequence and names of stages can vary. This list is from Part 1.

Tracking the status of problems also includes recording the identities of those responsible for problem resolution throughout each stage and cascading information to interested parties.

Effective problem management includes the use of information that assists root cause identification. For example:

- asset and configuration management information;
- change management records and reports;
- known error and workaround information, including from suppliers;
- information on similar problems.

Problem prevention spans individual incidents, e.g. repeated difficulties with a particular feature of a system through to strategic activities. The latter can require major expenditure to implement, e.g. investment in a better network. At the strategic level, problem management merges into the proactive aspects of availability management.

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

☒ Possible problems

- Services are at risk if problem management neglects the identification and resolution of root causes.
- Insufficient or inaccurate information on incidents and problems limits problem management to little more than incident resolution.
- Consideration being given only to short-term benefits of a workaround undermines the quality of the service and increases the service costs.

Service request management/Request fulfilment

A formal request from a user to a service provider is recorded on a service request. The activities to fulfil a service request depend on the type of request. Some service providers handle service requests using a special category of incident record. This is one of the reasons that Part 1 combines incident and service request management. Whatever approach is adopted incidents and service requests may have different targets.

Tracking service requests through their life cycle supports an effective process and allows reporting on the status of requests. Part 1 requires the service provider to keep the customer informed of the progress of their service request. This will usually impact customer and user satisfaction. If service targets cannot be met, customers need to be informed. Where necessary a service request is escalated according to a procedure.

ITIL provides guidance on a request fulfilment process that is separate from incident management. Separation enables standardization and automation that can reduce costs and results in better outcomes for users and customers. Reporting is often more meaningful.

Request fulfilment manages service requests from the initial service request to fulfilment. A request model defines any prerequisites, approvals needed and standard activities to fulfil the service request. As part of a request model, change requests can be required to complete the fulfilment.

Service requests that occur repeatedly are opportunities for automation and improvement, e.g. automating password reset requests. Each type of record should be clearly defined within an organization and have a standard workflow such as the examples shown in Figure 21.

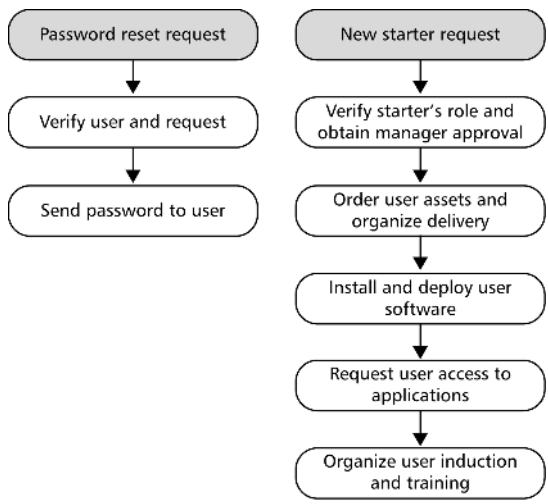

Figure 21 – Two types of service request model

A service provider can often centralize some fulfilment work to gain economies of scale, procurement and asset management. A self-service portal can be used with interfaces directly to procurement, finance and service management applications.

Chapter 12 Control processes

Introduction

The control processes collectively enable a service provider to maintain the integrity of the service configurations and accurate information to be used by the whole of the SMS as shown in Figure 22.

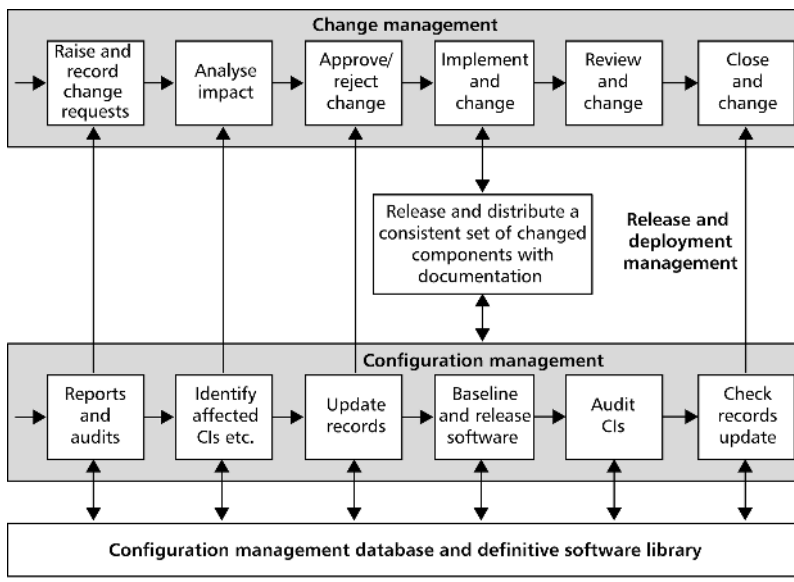

Figure 22 – How the control processes work together

Configuration management

Scope

Configuration management controls information on components managed by change management, release and deployment management. Components are referred to as configuration items (CIs).

A policy defines what is classed as a CI, e.g. services, systems, products, hardware, software, licences, documentation. CIs are documented in sufficient detail to support other processes, e.g. the ability to diagnose the root cause of a problem or impact analysis in change management. Configuration management and data should be integrated with those of its customers and suppliers to ensure that accurate information is available for changes and releases.

Managing configuration data and information

Configuration management information is maintained in a repository, often called a configuration management database (CMDB). In large installations there may be several databases or data sources. They comprise a logical CMDB or configuration management system (CMS). Reporting tools can combine information from multiple physical sources.

Information on CIs is held, used and managed through all stages: receipt, acceptance, installation, operation, maintenance, disposal and then retirement.

CI information is updated when:

- new CIs are registered;
- CIs are deleted/withdrawn or disposed/retired;
- software or data is moved, e.g. from one server to another;
- the state of a CI changes;
- CIs are updated;
- change requests and records are updated;
- releases are built, tested or deployed;
- location names change (e.g. new building).

If limited resources mean configuration management information is inaccurate, it is advisable to reduce the scope and level of detail.

Access controls should ensure staff have the correct level of access to the CMDB, physical hardware, software, media and documentation.

Planning

Planning defines a framework of scope, objectives, policies and procedures. It includes:

- an appropriate level of automation;
- provision of one or more CMDBs or other definitive source of information;
- secure libraries and storage for definitive masters and spares;
- staff trained in the processes and tools;

- identifying and labelling all assets and configuration items with any necessary relationships;
- identifying the location of a CI;
- linking CIs to services, service catalogues, SLAs, contracts and other formal agreements;
- establishing and maintaining baseline configurations;
- managing CI information;
- an approach to the control of all changes to CIs;
- CI status accounting and reporting;
- providing accurate configuration information to interested parties;
- configuration audit and verification.

☑ Benefits

- Consistent, cost-effective and repeatable management of CIs.
- Improved effectiveness, stability and security of the SMS and services.
- Management and protection of assets.
- Contribution to compliance with legal, regulatory and contractual obligations, e.g. controlling licences and preventing use of illegal software.
- Better control of changes and releases, including new or changed services.
- Provision of useful information for problems to be prevented or resolved more quickly, improved resource planning and financial management.
- Improved speed and accuracy of configuration audits.
- Improved control, security and disaster recovery.

Selecting and identifying CIs

CIs are selected and defined by subdividing the service into components. Service components are logically related hardware, software, services or combinations of these. Subdivision is based on criteria defined in the policy, e.g. safety or mission critical, high risk, logistics, ease of maintenance. CIs are defined by their service performance, functional and physical characteristics.

Information about a CI includes: CI identity, description, type, purpose, version, size, location, components, relationships to other configuration items and status.

Subdividing into too many CIs will complicate management and increase costs. Subdividing into too few CIs will create logistic and maintenance difficulties and limit control. The scope and degree of control should match the business needs.

Configuration control

Configuration control works with change, release and deployment management to ensure that only authorized and identifiable CIs are used and that the CMDB is updated.

Status accounting and reporting

Status accounting provides reports on different perspectives of CIs for different purposes. For example, an application support team will want to see individual application modules when fixing software problems. In contrast, a service desk will want to track and report incidents and problems against the main application release. Typical status accounting reports are included in Appendix D.

Configuration audit and verification

At appropriate intervals audits and verification should ensure that:

- there is adequate control of the configurations, e.g. unauthorized changes are detected;
- the configuration information accurately defines the actual physical configurations;
- the actual performance, usability, functionality and physical attributes of a CI meet the specification.

Finding a discrepancy quickly saves time and reduces problems and embarrassment, e.g. verifying that planned CIs are complete before a release is deployed. Automation can significantly reduce the costs of auditing configurations, e.g. desktop configurations. Superfluous software, licences and equipment are often found during audits and their removal can reduce costs. The increase or decrease in discrepancies and nonconformities provide a measure of the effectiveness of the process.

☒ Possible problems

- Immature culture; lack of understanding of what is involved.
- Lack of management commitment and support.
- An overly complex approach means records are difficult to keep current.
- Over-reliance on resource intensive manual processes, so the process is inefficient and error prone.
- CIs are defined in too much detail for the resources available.
- Difficulty defining owners of CIs and associated configuration data.
- Lack of adequate tools.

Change management

Scope

Change management maximizes the benefits of changes while minimizing disruption to service. Badly managed changes can result in service failure and degradation. Rework and unplanned activities usually waste resources.

Most services and systems are heavily interrelated so a change made in one part of a service can have profound impacts on another part. Change management is therefore integrated with configuration management so that changes to interrelated components are understood.

Changes to services can arise in response to problems and changes in requirements. For example: business, technology, policy or legislative requirements; or improvements to the SMS or service.

Change management includes the approach for:

- recording and classifying change requests by type;
- assessing the urgency, priority, cost and benefits;
- impact analysis and risk of each change;
- grouping changes (e.g. as a release, when this is beneficial);
- authorization, based on the type of change;
- change implementation;
- testing, verifying and signing off;
- reviewing the change;
- closing the request record.

Types of changes

Different types of changes are managed differently. For example a routine, standard change, done many times before, is managed more simply than a more complex change not done before. The same types are managed in the same way across the whole organization, even if some changes are controlled locally.

Emergency changes are a special type of change. They follow the activities of the normal process, although usually faster. When it is unavoidable, some details are documented retrospectively. Emergency changes are reviewed to check that there was a real emergency and not a failure to follow the correct process.

☑ Benefits

- Better alignment of services to actual business needs from faster and more reliable changes.
- Changes that maximize business benefit are given high priority.
- Reduction in the rate of failed changes or changes that are backed out.
- Visibility of changes across distributed enterprises.
- Prevention of uncontrolled change that causes disruption.
- Changes can be reversed or remedied to a previous state.

Understanding changes

Each change record is given a unique reference and includes:

- the name of the person raising the change;
- a description and identification of affected configuration items and versions;
- expected classification of the type of change (e.g. emergency, high, normal, low);
- relationship between a change and other proposed or planned changes;
- the expected impact of the change (e.g. major, minor impact);
- reference to supporting documents (e.g. known errors, purchase orders, other changes);
- the reason for the change, i.e. the justification and business benefits;
- resources to analyse and implement the change.

Useful information is produced by change management, either via direct access to the information by people performing other processes, or via

reports. Examples are a service desk having information on what changes happened in the last week and what changes are planned. Typical reports are listed in Appendix D.

Change approval and change advisory boards

A change authority considers requests for change and makes recommendations on whether a change should be accepted or rejected. The change authority can be a person, e.g. a change manager, or a group, often referred to as a change advisory board (CAB). Each affected party assesses the risk, impact and business benefit of each change and contributes to the overall approval or rejection of a change request.

The levels of authorization for each type of change should be based on the impact and risk for each type so that higher risk changes require a higher level of seniority to authorize. For example, changes that affect many sites are approved by a global change board or board of directors.

Physical meetings are useful for the highest risk changes. Information on the changes is provided with enough time for consideration to be given to them. An agenda should be circulated and decisions documented.

Scheduling and implementing a change

A schedule of changes should be maintained and made available to those involved in either approval of the change or those that are affected by the change. The schedule should avoid a clash between the change and a business critical period. Changes that require the service to be down during normal hours should be agreed with those affected well in advance. The changes should only be made during the time shown in the schedule.

Closing and reviewing the change request

Changes are reviewed after implementation and any additional, unplanned actions required noted. For significant changes a more detailed review is required, although the principles are the same. Lessons learned from reviews should be fed back into future changes or a plan for improving the service. After a change has been successfully implemented final updates of records are made, including actual resources used and costs incurred.

☒ Possible problems

- The process is too bureaucratic.
- Lack of support from managers means the procedure is not followed.
- The scope of a change is too wide for the resources available.
- Inaccurate information on the change requested results in delays and inaccurate assessments.
- Too many dependencies make changes difficult to schedule.
- Back-out procedures are missing or untested.
- The procedure is manually intensive.
- The emergency change process is abused.

Release and deployment management

Scope

A release is a set of changes to CIs and/or new CIs. A key feature is that linked changes are planned, tested and implemented into the live environment at the same time. Release and deployment management coordinates the activities of several groups, including suppliers and customers.

The process is integrated with change and configuration management to ensure the CMDB is up to date.

The basis for creating a release is:

- a release policy on types of release and what changes constitute a release;
- planning release creation and deployment,
- use of information from the CMDB;
- developing or acquiring software;
- registering master copies of software and electronic assets;
- hardware and spares;
- designing and preparing the release;
- deployment;
- verification and acceptance of the release.

Release policy

The procedure followed for release and deployment varies according to the type of release. A release can be simple or complex. The release of a website update used by millions can be much simpler than a complex software release for a single business unit.

A release policy can be used to define the key aspects of release and deployment and should be agreed with stakeholders. The policy includes:

- type of release and expected frequency;
- roles, responsibilities and authority levels for all stages of the process;
- the business critical times when a release should be avoided;
- the approach to grouping changes into a release;
- methods of release identification, unique versioning and description;
- methods for the build, installation, release and deployment;
- verification and acceptance after deployment.

☑ Benefits

- Minimizes disruption and risk to the business.
- Reduces risks as closely interrelated components are tested together.
- Enables a batch of changes to be deployed quickly and cost-effectively.
- Provides a reliable mechanism for repeated deployment.
- Sets expectations on what will happen.
- Problem, change and configuration management records are updated efficiently and in a timely manner.

Release and deployment planning

Good planning and management are essential to deployment of a release, including managing the risks to the customer and services. The deployment of a release may be phased, e.g. by location.

Plans should cover what, how, when and who will do what. Planning should use information from the CMDB to ensure all changes in the release are compatible. Consideration should be given to what needs to be in place before the release can be deployed, including documentation, training, timing and notification for support staff. Extra support resources should be planned during major upgrades to ensure that the service levels are maintained. The plans should include how progress will be tracked and reported.

Secure storage areas are required for software and hardware. Removal of redundant products, services and licences should be planned for.

The plans should be agreed and communicated to those involved and those affected.

Design, build and configure release

Release and deployment should be compatible with the architecture, standards and business processes, e.g. procurement. It is best practice to package the release components into a release package that is registered in the CMDB. It is important to verify configurations during the process, e.g. checking that the target platform satisfies prerequisites before installation. Using a template-driven approach and automating the process reduces errors and ensures that the process is repeatable and faster.

It is important that information relevant to statutory, regulatory or contractual obligations is kept up to date, for example, software licence information.

Deliverables from the build activity, e.g. release note or installation instructions should be available during testing. The build inputs and outputs are placed under configuration management and stored in a secure environment to enable recovery from disaster or failed changes.

Deployment

Deployment usually includes other processes and several functions within the organization, e.g. logistics, health, safety and electrical checks.

After deployment of a release configuration information should be updated so that other staff can resolve incidents and problems more efficiently. The number of incidents related to a release in the period immediately following a deployment should be monitored. The results should be analysed to assess the impact of the incidents on the business, operations and support staff resources.

Supporting documentation should be controlled and accessible, e.g. release documents, service documents, support procedures and licences.

Verification and acceptance

Verification and acceptance occurs at each stage of release and deployment. A person with the correct level of authority should sign off each stage of acceptance testing, including the final stage for the whole release against the requirements. Sign off should only occur after adequate testing. Key staff and users should be involved in verification of the requirements and during the acceptance phases.

Verification should show that a release is complete and correct before and after deployment and that the CMDB has been updated. If there are defects outstanding after deployment incident management should be

informed of known errors and workarounds. If the release is rejected, delayed or cancelled, change management should be informed.

Change management should include a post-implementation review for the whole release deployed. Users often perform a final acceptance test of the installed software, e.g. a desktop upgrade. A post-installation satisfaction survey is useful to provide feedback.

☒ Possible problems

- A lack of understanding of who is responsible for what at each stage.
- Confusion about the scope of and interfaces between all three control processes.
- Insufficient staff, machine and network resources to build and test new releases.
- Insufficient resources available for acceptance testing.
- Test results are partially acceptable, e.g. parameters not set the same.
- A lack of understanding of the release contents, build and installation components and their interdependencies, leading to mistakes.
- Insufficient local control of components involved in or affecting the release.
- Incorrect assumptions during planning for deployment across different cultural and geographical groups.
- Staff reluctant to back out a release and there is pressure to accept a defective release.
- Staff misunderstand the business requirements or timescales.
- Staff unable to handle any unexpected events.

Chapter 13 SMS Automation

Introduction

The range and sophistication of automated solutions and tools for service management have grown rapidly in recent years. Accessing service management information remotely allows the service provider to use the most effective locations, allowing either centralization or decentralization.

Typical solutions

Typical types of service management solutions to support the core processes are:

- service desk or help desk, with or without a CMDB;
- integrated service management tools;
- technology such as computer telephone integration (CTI), voice over internet protocol (VOIP), interactive voice response systems (IVR);
- the internet, e-mail, voicemail, fax;
- messages and calls to mobiles, personal digital assistants;
- self-help knowledge bases;
- search engines and systems;
- remote diagnostic tools;
- workflow capability to manage and track progress;
- automated system and network management;
- automated event management, alerting and escalation capabilities;
- remote release and distribution;
- configuration discovery, collection and audit tools;
- security monitoring and control, including password control, detection of violations and virus protection;
- performance and capacity planning;
- contingency management (including automatic backups);
- reporting and visualization tools that access several databases.

The Internet and intranets provide useful facilities for service management in global, local and distributed environments. These include:

- general marketing;
- e-mail;

- self-service portals;
- supplier program fixes and upgrades;
- publishing of known errors;
- customer notice-boards;
- frequently asked questions (FAQs);
- knowledge searches;
- access to automated service reporting;
- a common cross-platform user interface;
- software fixes that can be downloaded either by support staff or by the customers themselves;
- access and searching of solutions to problems, known errors and fixes, to reduce problem-solving time.

☑ Benefits

- Reduces costs by reducing repetitive manual tasks.
- Improves the cost-effectiveness and speed of service management processes.
- Provides cost-effective control of the services and configurations.
- Enables the centralization of key functions with fewer administrators.
- Improves the analysis of raw data and the identification of trends.
- Enables the implementation of preventive measures.
- More predictable outcomes by the use of estimation, modelling and simulation tools.

Selecting and implementing automated solutions

Each application or tool for the automation of service management has advantages and disadvantages. For a very small service provider a simple database system can be sufficient for logging and controlling incidents. However, in a very large service provider, a sophisticated, distributed, integrated service management toolset can be required, linking all processes with event-management systems. Workflow management provides a communications backbone for service management in large service providers (e.g. to link each task in the life cycle from a new service being planned through to disposal). However, after a merger, a major reorganization or a change to the SMS the workflow states can need to be re-engineered to support other groups with existing data.

The following should be borne in mind when considering automation:

- percentage fit to operational requirements;
- the meeting of all mandatory requirements;
- the ease of use for all stakeholders;
- the fit with the existing and planned technical platforms, architectures and strategies;
- a sound data and information structure;
- scalability;
- flexibility;
- process capability (e.g. support for best practices described by ITIL, or COBIT and the ISO/IEC 20000 series);
- the measurement framework (e.g. support for of objectives, goals and metrics described in ITIL and COBIT);
- management information and performance reporting;
- integration capabilities (e.g. process and information integration such as the ease of flow of data and control between processes);
- the ability to interface other tools (e.g. reporting and visualization tools);
- support for multiple languages;
- visualization (e.g. configuration of a network);
- the ability to load information automatically (e.g. from audit and discovery tools);
- acceptable levels of tool customization;
- administration and maintenance costs within budget;
- current user base and feedback from reference sites;
- ability of the supplier to deliver a solution and provide support;
- costs of the product, training, consultancy, maintenance and utilization.

With service management automation it is important to ensure that the combination of technology, processes and people are integrated and meet the needs of the users and customers. Automation should be used to enhance service management, not replace it. To select and implement automated solutions it is good practice to use a project management method as this ensures the technology, data, people and process changes are implemented together.

Practical success factors for automation

To successfully automate service management and implement tools it is important to:

- use a good project management method;
- define the objectives and requirements for automation;
- design the solution within the context of the SMS;
- get buy-in from the relevant stakeholders and staff;

- have formal selection and weighting criteria;
- consider parallel running of old and new tools taking into account the management overhead and other costs;
- phase the implementation with feedback sought at each stage;
- accommodate integration with other tools and databases;
- ensure look-up lists are short, meaningful and concise;
- look for simple tools or process improvements for gaps discovered during development and implementation.

☒ Possible problems

- An unrealistic expectation of the tool leads to loss of enthusiasm.
- Workflow set-up is seen as too bureaucratic and the tool is blamed.
- Sophisticated tools introduced into service providers with an immature culture will be used only partly and possibly badly, incurring costs but delivering only some of the benefits expected.
- Inadequate resources for the implementation, particularly staff implementing tools while also doing their operational jobs.
- Implementation of tools provides poor support for process integration.
- Tools selected impose an unsuitable process.
- Data for a replacement tool cannot be converted.
- A faulty or immature process remains defective when automated.
- Failure to train staff adequately in the use of the tools.

Appendix A Terms and definitions

The terms and definitions given below are mainly taken from ISO/IEC 20000-1:2011, Clause 3. Where terms and definitions are from another source this is indicated. All other words in the 20000 series and this book are used in their normal meaning as included in commonly available English-language dictionaries.

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

NOTE 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.

configuration baseline
configuration information formally designated at a specific time during a service or service component's life

NOTE 1 Configuration baselines, plus approved changes from those baselines, constitute the current configuration information.

NOTE 2 Adapted from ISO/IEC IEEE 24765:2010

configuration item
CI
element that needs to be controlled in order to deliver a service or services

configuration management database
CMDB
data store used to record attributes of configuration items and the relationships between configuration items, throughout their lifecycle

continual improvement
recurring activity to increase the ability to fulfil service requirements

NOTE Adapted from ISO 9000:2005.

corrective action
action to eliminate the cause or reduce the likelihood of recurrence of a detected nonconformity or other undesirable situation

NOTE Adapted from ISO 9000:2005.

customer
organization or part of an organization that receives a service or services

NOTE 1 A customer can be internal or external to the service provider's organization.

NOTE 2 Adapted from ISO 9000:2005.

document
information and its supporting medium
[ISO 9000:2005]

EXAMPLES Policies, plans, process descriptions, procedures, service level agreements, contracts or records.

NOTE 1 The documentation can be in any form or type of medium.

NOTE 2 In this International Standard, documents, except for records, state the intent to be achieved.

effectiveness
extent to which planned activities are realized and planned results achieved

[ISO 9000:2005]

external organizations
used in Part 1 in the normal English language sense, for any organization that has access, uses or manages the service provider's information or services. This usage is specific to information security and relates to the agreement and operation of controls to protect the service provider's information

governance
system by which organizations are directed and controlled

normal English language meaning

governance of IT
responsibility of executives and the board of directors and consists of the leadership, organizational structures and processes that ensure that the enterprise's IT sustains and extends the organization's strategies and objectives

governance of processes operated by other parties
direction, control and evaluation of those organizations or parts of organizations that contribute to the service by operating processes or parts of processes

Not a Part 1 definition, based on text and the intentions of the ISO/IEC 20000 series

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

information security
preservation of confidentiality, integrity and accessibility of information

NOTE 1 In addition, other properties such as authenticity, accountability, non-repudiation and reliability can also be involved.

NOTE 2 The term 'availability' has not been used in this definition because it is a defined term in this part of ISO/IEC 20000 which would not be appropriate for this definition.

NOTE 3 Adapted from ISO/IEC 27000:2009.

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

[ISO/IEC 27000:2009]

interested party[3]
person or group having a specific interest in the performance or success of the service provider's activity or activities

EXAMPLES Customers, owners, management, people in the service provider's organization, suppliers, bankers, unions or partners

NOTE 1 A group can comprise an organization, a part thereof, or more than one organization.

NOTE 2 Adapted from ISO 9000:2005.

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 a service or services

NOTE The internal group is outside the scope of the service provider's SMS.

[3] Part 1 refers to 'interested parties' and uses it in the same way as other best practices use 'stakeholder'. The normal English language meaning of 'stakeholder' includes: 'someone who has an interest'.

known error
problem that has an identified root cause or a method of reducing or eliminating its impact on a service by working around it

major incident
serious disruption to normal service, the definition of which is agreed between the service provider and customer

Not a Part 1 definition, but based on its intent.

nonconformity
non-fulfilment of a requirement

[Taken from ISO 9000:2005]

organization
group of people and facilities with an arrangement of responsibilities, authorities and relationships

EXAMPLES Company, corporation, firm, enterprise, institution, charity, sole trader, association, or parts or combination thereof.

NOTE 1 The arrangement is generally orderly.

NOTE 2 An organization can be public or private.

[ISO 9000:2005]

other parties
suppliers (including lead suppliers), internal groups and customers (acting as suppliers), all of whom contribute to the operation of the SMS and delivery of the service but who are not part of the service provider's organization

Not a Part 1 definition, but based on its intent.

preventive action
action to avoid or eliminate the cause or reduce the likelihood of occurrence of a potential nonconformity or other potential undesirable situation

NOTE Adapted from ISO 9000:2005

problem
root cause of one or more incidents

NOTE 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.

procedure
specified way to carry out an activity or a process

ISO 9000:2005

NOTE Procedures can be documented or not.

process
set of interrelated or interacting activities which transforms inputs into outputs

[Taken from ISO 9000:2005]

process owner
this is not used in the 2011 edition of Part 1, although it is commonly used in the service management industry to describe managers that are responsible for the quality and effectiveness of a process. This role is based on responsibility and levels of authority delegated by the Part 1 responsible manager

record
document stating results achieved or providing evidence of activities performed

[ISO 9000:2005]

EXAMPLES Audit reports, incident reports, training records or minutes of meetings.

release
collection of one or more new or changed configuration items deployed into the live environment as a result of one or more changes

request for change
proposal for a change to be made to a service, service component or the service management system

NOTE A change to a service includes the provision of a new service or the removal of a service that is no longer required.

responsible manager
(often referred to as service owner) is a Part 1 term that is used in its normal English language sense, i.e. not a special term. This manager has authority over and is responsible for many aspects of the SMS and service, e.g. ensuring the service requirements are input to the SMS. In Part 1, the authority levels and responsibilities are normally delegated by the 'top management'

risk
effect of uncertainty on objectives

NOTE 1 An effect is a deviation from the expected – positive and/or negative.

NOTE 2 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).

NOTE 3 Risk is often characterized by reference to potential events and consequences, or a combination of these.

NOTE 4 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.

[ISO 31000:2009]

service
means of delivering value for the customer by facilitating results the customer wants to achieve

NOTE 1 Service is generally intangible.

NOTE 2 A service can also be delivered to the service provider by a supplier, an internal group or a customer acting as a supplier.

service catalogue
database or structured document with information about all live services, including those available for deployment. The service catalogue is part of the service portfolio and contains information about two types of IT service: customer-facing services that are visible to the business; and supporting services required by the service provider to deliver customer-facing services

Taken from ITIL, © Crown copyright 2011, Cabinet Office

service component
single unit of a service that when combined with other units will deliver a complete service

EXAMPLES Hardware, software, tools, applications, documentation, information, processes or supporting services.

NOTE A service component can consist of one or more configuration items.

service continuity
capability to manage risks and events that could have serious impact on services in order to continually deliver services at agreed levels

service level agreement
SLA

documented agreement between the service provider and customer that identifies services and service targets

NOTE 1 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.

NOTE 2 A service level agreement can be included in a contract or another type of documented agreement.

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

service management
a set of specialized organizational capabilities for providing value to customers in the form of services

Taken from ITIL © Crown copyright 2011. Cabinet office.

service management system
SMS
management system to direct and control the service management activities of the service provider

NOTE 1 A management system is a set of interrelated or interacting elements to establish policy and objectives and to achieve those objectives.

NOTE 2 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.

NOTE 3 Adapted from the definition of 'quality management system' in ISO 9000:2005.

service pipeline
database or structured document listing all IT services that are under consideration or development, but are not yet available to customers. The service pipeline provides a business view of possible future IT services and is part of the service portfolio that is not normally published to customers

Taken from ITIL, © Crown copyright 2011. Cabinet Office.

service portfolio
complete set of services that is managed by a service provider. The service portfolio is used to manage the entire lifecycle of all services and includes three categories: service pipeline (proposed or in development), service catalogue (live or available for deployment) and retired services

Taken from ITIL, © Crown copyright 2011.Cabinet Office.

service provider
organization or part of an organization that manages and delivers a service or services to the customer

NOTE 1 A customer can be internal or external to the service provider's organization.

service request
request for information, advice, access to a service or a pre-approved change

service requirement
needs of the customer and the users of the service, including service level requirements and the needs of the service provider

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

NOTE Suppliers include designated lead suppliers but not their sub-contracted suppliers.

top management
person or group of people who direct and control the service provider at the highest level

NOTE Adapted from ISO 9000:2005.

transition
activities involved in moving a new or changed service to or from the live environment

Appendix B Agreements with the customer

Part 1 Clause	Agreement
4 Service Management system general requirements	SMS in place and agreed with the customer. This acts as the basis for changes and improvements in the SMS and services.
5 New or changed services	Plans, designs, acceptance criteria and the actual new or changed services and any other documents affected by the new or changed service being introduced.
6.1 Service level management	A catalogue of services, services to be delivered, including dependencies between services or service components, one or more SLAs taking into consideration all service requirements. Contact details (see Appendix C).
6.2 Service reporting	Service reporting requirements of the customer (as one of the interested parties).
6.3 Service continuity and availability management	Service continuity requirements and availability requirements, for both after a major service loss and normal service. This takes into account applicable business plans, service requirements, SLAs and risk. They should include at least user access to services (also compliant with an information security policy), service response times and end-to-end service availability. Plans and the results of tests of plans for service continuity and availability are also required. It can be advisable, although not compulsory, to agree the plans with the customer.
6.4 Budgeting and accounting	No requirement for agreement with the customer. However, it is advisable to agree with the customer the basis on which costs are tracked, especially if services are charged for.

Part 1 Clause	Agreement
6.5 Capacity management	Capacity and performance requirements agreed with the customer (and interested parties). Interested parties have a specific interest in the performance or success of the service provider's activities. For example, owners, people in the service provider's organization, or partners.
6.6 Information security	No service requirements to be agreed with customers, although the service requirements are taken into account when the information security policy is being developed.
7.1 Business relationship management	Service requirements and changes to service requirements may be identified by BRM, changed under the control of change management, but BRM do not agree the service requirements with the customer (see 6.1 Service level management). The definition of a service complaint is agreed with the customer.
7.2 Supplier management	The service provider and the supplier shall agree a documented contract. This does not involve the customer, but supports the service required by the customer. The service provider shall agree with the supplier service levels to support and align with the SLAs between the service provider and the customer (but not agree this with the customer).
8.1 Incident and service request management	No requirements for agreements with customers in Part 1. Many features influencing this process(es) are agreed as part of service requirements by SLM and other processes, e.g. target fix times, contact details.
8.2 Problem management	Nothing agreed directly. Some features influencing this process(es) will be agreed as part of service requirements by SLM. For example, target fix times.
9.1 Configuration management	Nothing agreed directly. Some features influencing this process(es) will be agreed as part of service requirements by SLM and other processes. For example, the change management policy.
9.2 Change management	Nothing agreed directly with the customer under Part 1 requirements. Some features influencing this process(es) will be agreed as part of service requirements by SLM and other processes. The service provider and interested parties (which can include customers) shall make decisions on the acceptance of requests for change.

Part 1 Clause	Agreement
	Decision-making shall take into consideration the risks, the potential impacts to services and the customer, service requirements, business benefits, technical feasibility and financial impact. A schedule of changes containing details of the approved changes and their proposed deployment dates shall be established and communicated to interested parties (which can include customers). A schedule of changes is established and used as the basis for planning and communicating the deployment of releases. The service provider shall review changes for effectiveness and take actions agreed with interested parties (which can include customers).
8.3 Release and deployment management	The service provider shall establish and agree with the customer a release policy stating the frequency and type of releases. The service provider shall plan with the customer and (other) interested parties the deployment of new or changed services and service components into the live environment. The service provider agrees with the customer the definition of an emergency release. Acceptance criteria for the release shall be agreed with the customer and interested parties.

Appendix C Guidance on SLAs

Defining the SLA structure

It is important that the structure of the master and the individual SLAs is agreed with customers early in their development. For example should there be one or many SLAs? What level of detail is required by the customers? And what service targets are the most appropriate representation of the customer's business requirements?

The SLA structure should be manageable for the SLM function and should meet customer's business requirements, taking into account:

- geographical placement;
- organizational structure and management hierarchy;
- number and types of business groups;
- differences in services required inter- and intra-business groups;
- frequency of changes to the SLA;
- the structure should be agreed by the supplier and customer management.

Contents of a sample SLA

It is usually preferable to include references to other documents in each SLA rather than include detail common to several SLAs, e.g. procedures common to several services. It is counter productive to include a large number of targets or workload measures.

A large number of targets can distract attention from those that describe business critical components of the service.

The cost of monitoring and reporting on a wide range of service issues can outweigh the benefits and will be seen as an unacceptable overhead. A master SLA can be used for this purpose. The non-prescriptive list is included to prompt the development of an SLA that is appropriate to the service(s) in question. This list should not be used in its entirety as the basis for an SLA.

The SLA can include some of the following information according to the service in question:

- a brief service and business critical issues description;
- validity period and/or SLA change control mechanism;
- authorization details;
- a brief description of communications, including:
  - contact points;
  - communications channels/methods;
  - reports and service reviews/references (to other processes).
- names and means of contacting people authorized to act in emergencies by participating in problem correction, recovery or workaround;
- service hours, e.g.:
  - 9:00 to 17:00;
  - date exceptions (e.g. weekends, public holidays);
  - critical business periods.
- scheduled and agreed interruptions, including:
  - type and notice to be given;
  - number per period.
- customer responsibilities such as:
  - delivery of input media;
  - response to instructions to log off at end of day;
  - protection of security identities;
  - control of the media on the desktop.
- service provider liability and obligations, e.g.:
  - security;
  - impact and priority guidelines;
  - escalation and notification process;
  - complaints procedure.
- service targets, e.g.:
  - system response times;
  - reliability/availability (is it available when it is needed?).
- workload limits (upper and lower), e.g. the ability of the service to support the agreed number of customers/volume of work, system throughput;
- high-level financial management details, e.g. charge codes, etc.;
- action to be taken in the event of a service interruption;
- housekeeping/data security, including how this is achieved and how the service is affected by it;
- glossary of terms;
- supporting and related services;
- any exceptions;
- statement of the supplier's obligations regarding such matters as:
  - report production schedule;
  - on-line availability and performance;
  - fault response;
  - recovery times for various types of failure.
- functionality (i.e. does the system do all the right things correctly);
- disaster recovery;
- charging/budget details.

Guidelines for service level targets

The guidance given below does not preclude the use of different measures within an individual SLA, if appropriate.

Targets to consider were highlighted in the description of the SLA structure. Any of the measures listed as reports in Appendix D could be used as a target in an SLA. Targets should not be included in the SLA unless they can be monitored and reported with adequate accuracy but without excessive costs being incurred. Choice of targets should also take into account which aspects of the service matter most to the customers.

The same reasoning applies to SLAs, OLAs and external, legally binding contracts. The following should be determined:

- whether the targets and workload measurements are concise and relevant to customer's business needs;
- whether the targets and workloads measurements are objective and cost-effectively measurable;
- whether any targets are potentially ambiguous (e.g. is the method of calculating availability understood by both supplier and customers?);
- whether any of the targets are duplicates because they cover the same or similar aspects of the service;
- whether the targets and workload measurements incorporated into the individual SLAs will be easily understood so that they can be used as part of the SLM process.

Appendix D Service management reports

It is not useful to produce a large number of reports, even if a lot of data is actually available from monitoring. Too many reports can confuse the reader. The following list gives examples that could be used to select a subset of reports that are of interest.

Workload and problem management reports

- Telephone calls and emails/electronic messages:
  - number and percentage of inbound and outbound;
  - number of calls per support person receiving calls, also as a percentage of all calls, per support person;
  - queue times;
  - number and percentage of abandoned calls;
  - number and percentage switched through to voicemail;
  - number and percentage of picked up in x seconds;
  - wait time to call pick-up;
  - staff performance;
  - staff availability to take telephone calls;
  - duration;
  - profile throughout day, week, month, year;
  - out of hours.
- Number and percentage of calls/requests logged of types:
  - incident/problems;
  - service requests;
  - changes.
- Number and percentage of calls/requests logged in each status, e.g. logged, resolved, closed.
- Number and percentage of resolved calls/requests and (separately) outstanding calls/requests, by:
  - location/time zone;
  - business area;
  - type;
  - severity and priority;
  - service provider (including suppliers);
  - problem solver;
  - overall.

- Number and percentage of calls/requests resolved on the telephone or by prompt return communication:
  - overall;
  - by service provider;
  - by problem solver.
- Number and percentage of calls/requests not acted upon within agreed service levels, broken down by:
  - call type (especially the most common types);
  - resolving group;
  - customer business area;
  - severity.
- Number and percentage of calls/requests received per period and per customer business area by:
  - category;
  - severity;
  - CI.
- Number, percentage and types of escalated calls/requests.
- Type of requests consuming the most service provider or supplier resources.
- Type of requests taking the longest time to turn around to customers.
- Customers, applications and equipment requiring the most support.
- Type of requests causing the highest business impact and associated costs.
- Customer satisfaction and perception.
- Identified training needs for:
  - customers;
  - support groups;
  - individual staff;
  - CI (e.g. specific application, type of hardware).

Financial reports

Financial reports should include:

- total costs and total charges against budget comparisons;
- values of assets and the cost of depreciation;
- cost per service unit, with units such as:
  - per problem;
  - per customer;
  - per item of hardware, e.g. a PC;
  - per unit of storage;
  - true cost of service or technology ownership.

Asset and configuration management reports

Asset management reports should include:

- number of assets by type (including software licences);
- value of assets;
- location of assets and assets by business units.

Configuration management reports should include:

- selected CIs and their components;
- version and status;
- associated documentation;
- dependencies and related changes and problems;
- all the components in a service system:
  - change;
  - baseline;
  - build or release;
  - version or variant, e.g. build or baseline list.
- current and historical data for each CI as it has progressed through its life cycle, e.g. through:
  - ordered;
  - received;
  - in acceptance test;
  - live;
  - under change;
  - withdrawn;
  - disposed.

CIs that change frequently require high levels of support or cause many incidents and outages for the business.

A report for a CI can include the unique label, description, current status, owner responsible for change, change history, open problems/requests for change.

Change management reports

Change management reports can include all or some of the following:

- number of change requests;
- number and percentage of changes that were:
  - rejected;
  - emergencies;
  - in change status.
- number and percentage of changes awaiting implementation by:
  - category;

  - time outstanding.
- number and percentage of implemented changes by:
  - configuration component;
  - service.
- change backlogs and bottlenecks;
- costs per change and cost summaries;
- business impact of changes;
- changes by business area;
- frequency of change to CIs;
- status reports supporting service management activities, e.g. progress monitoring, problem management, change control, release management, configuration audits and service planning;
- information should also be available on the validity period of contracts, SLAs or service level objectives (SLOs) and the value of any services, including those provided by suppliers.

Appendix E Preparing for a Part 1 audit

Defining and maintaining the scope statement

When seeking certification a service provider should state the scope of the service to be audited and agree this with the auditor in advance of the audit. The scope statement should be confirmed by the auditor, referenced in the audit report and stated on any certificate of conformity. The scope statement should include at least the name of the service provider's organization and the services provided. Services should be 'all services' or named services. Other parameters can be used, as described in Chapter 4.

Those who wish to take assurance from a service provider's certificate ought to ask to see the certificate and scope statement. The audit certificate should not imply that the certified service provider has capabilities over and above those covered by the assessment. The auditor should also ensure that the declared scope accurately describes the actual scope of the assessment.

If at any time during a service provider's certification lifetime the auditor determines that the declared scope has changed, then the certificate and possibly the basis of the certificate will need to be amended.

The terms of a service contract cannot remove or reduce the obligation on the auditor to obtain sufficient appropriate evidence of conformity to the specified requirements. For example, if a contract between a service provider and a customer means a service management process is excluded from the service and from the SMS. This service provider cannot achieve Part 1 on the basis that missing processes are a contractual issue and as such it is out of their control that some services are not performed. This is because all requirements in Part 1 are compulsory and a contract cannot over ride rules on an acceptable scope for a certification audit.

A service provider can have other contracts and other customers that allow them to agree an acceptable scope statement for a Part 1 audit. As a result an audit may be scoped by several services, customers or locations. This type of scope statement is inevitably more complex to agree and document.

For some specialized service providers it will not be possible to demonstrate compliance with all the Part 1 requirements, as the nature of the specialization means some processes are not performed. This is rare, but when this is the case another standard will be more appropriate, for example ISO 9001.

A single certificate cannot be awarded to service providers that are formed from more than one legal entity, even if the service management processes cross the boundaries between them. This restriction applies whatever the basis of ownership of the organizations.

The certificate may be awarded to an organizational unit that forms part of a bigger, single legal entity. For example, a service provider that is the in-house IT department. This contrasts with a service provider being an entire single legal entity. That this service provider is part of a larger organization will be defined in the scope statement.

Seeking certification

The service provider is the organization that seeks certification.

The requirements of Part 1 are independent of the service provider's organizational form. However, if relevant processes are performed by units that are not part of the service provider's organization, certification might rely on a contribution by another organization.

The service provider should demonstrate their control over the relevant services delivered by other parties. This includes governance of processes operated by other parties, as described in Chapter 4. The service provider should also demonstrate that service levels and any other measures of service quality are monitored and reported objectively and meet the agreed needs of the customer.

Part 1 is not normally appropriate for service providers who do only a minority of the service management themselves.

A customer or other parties, such as suppliers, are not directly involved in an audit. This requires the service provider to demonstrate control of all processes, including those that cross organizational boundaries by providing suitable evidence.

The service provider must also be able to demonstrate acceptable practices (over time) for each requirement (i.e. the 'shalls'), to have evidence of effective integration of all processes (not just the service management processes) and to have effective continual improvements and demonstrable management commitment.

When more than one organization is involved

It is not necessary for all organizations in a supply chain to achieve Part 1 for the service provider to gain certification. The caveat is that the service provider should be able to demonstrate that they control their suppliers. This includes managing interfaces effectively and having control of the data that flows either way across the interfaces. However, where multiple organizations are involved, the following features apply.

- A service provider aspiring to certification is required to comply with the requirements for each process within the scope of ISO/IEC 20000. Alternatively, where the service provider seeking certification does not have direct responsibility for every process in the SMS it should be possible to demonstrate they have governance of the processes. The interfaces should be controlled by the service provider.
- If certification is sought by a service provider reliant on suppliers contributing to the attainment, the suppliers would not as a consequence of the contribution gain certification through this mechanism. The suppliers would have to be audited and found to be meeting the required standard for the service provider seeking certification to be successful. Only those processes that directly contribute to the service provider's certification should be included in the audit.
- Where a service provider seeking certification has a contract to supply services and their customer is in turn a supplier to another organization further down the supply chain, the service provider may still attain certification if the customer for those services contributes to the attainment. Gaining a certificate as a service provider in these circumstances is possible only if the contribution by the customer to the certification is included in the audit. The customer would not as a consequence of their contribution gain a certificate through this mechanism.
- If there are multiple suppliers and customers involved it is essential that the scope of the SMS is limited to only those where all the requirements are fulfilled. In some cases the scope will be limited to a specific service and a specific customer. The scope can be a range of services to several customers, including their own in-house colleagues. It will not be possible for a service provider to attain certification for all services or all customers on the basis of achieving the required standard for just one of the customers.
- Auditor(s) will decide the number of customers or locations that should be audited. This decision will be based on an understanding of the complexity of the arrangement, the variety of services offered and size of the service provider's organization.
- For the purposes of certification it is irrelevant which of the parties is defined in a contract (or SLA) as the supplier and which is defined as the customer. However, auditor(s) will use their judgement of the validity of the certification for a service provider that provides only

some of the service/service management processes. It will generally be appropriate for certification to be awarded only to a service provider that is the supplier of the majority of the service/service management processes.

- It is particularly important to make the scope unambiguous where multiple organizations contribute to the service management processes being audited.

Appendix F ITIL support for Part 1 requirements

The table shows how the ITIL books support Part 1. Although an ITIL process is generally described in only one of the core ITIL life-cycle books the process applies across many service life-cycle stages.

For each ITIL core publication the second column of the table shows the ISO/IEC 20000 clause that is supported.

ITIL process	Part 1 Clause	Comments
1. Service strategy book		
Strategy management	4. Service management system general requirements	The ITIL strategy management for IT services is the process of defining and maintaining an organization's strategy with regard to its services and the management of those services. It is broadly equivalent to parts of Clause 4, specifically defining the scope and planning the services and SMS. This covers activities by top management in particular. Many of the Part 1 service requirements come from strategy.
Demand management	4. Service management system general requirements 6.5 Capacity management 7.1 Business relationship management	The purpose of ITIL demand management is to understand, anticipate and influence customer demand for services and to work with capacity management to ensure the service provider has capacity to meet this demand. This includes all resources and capabilities for the SMS and those required to deliver the services. This supports Clause 4 as it enables a service provider to balance supply and demand, including Clause 4 resource management. ITIL

ITIL process	Part 1 Clause	Comments
		demand management also supports parts of Clause 4, for establishing the SMS and then improving it. 7.1 requires a more strategic view of service requirements, including an understanding of business activity changes that can affect the requirements for capacity and performance. ITIL can be used to provide advice on this clause.
Service portfolio management	4.1 Management responsibility 4.5.4.3 Management review Clause 5 Design and transition of new or changed services	The ITIL service portfolio management process tracks and approves investments in new services or changes to services as well additional capacity. It can also support 4.1, 4.5.4.3 and Clause 5.
Financial management for IT services	6.4 Budgeting and accounting for services	The ITIL financial management for IT services process can support 6.4. There are no requirements for charging in Part 1, so some ITIL financial advice is useful but does not support certification under Part 1.
Business relationship management	7.1 Business relationship management	The ITIL business relationship management process can support 7.1. Business relationship management has an overall more strategic view of service and service requirements than, for example, SLM, 6.1.

ITIL process	Part 1 Clause	Comments
2. Service design book		
Supplier management	4.2 Governance of processes operated by other parties 6.1 Service level management 7.2 Supplier management	The ITIL supplier management process can be used to support 7.2. However, the advice in ITIL is also relevant to 4.2. This clause is important for the service provider's ability to define the scope of the SMS, but also as a supplement to the requirements in 7.2 for supplier management. This is in part because there is a strong link between meeting the requirements of 4.2 and the terms of the contracts agreed with suppliers. Some aspects of ITIL supplier management also support the management of internal parties and customers acting as suppliers, who are referred to as part of the governance, but are managed under 6.1, under a documented agreement. For customers acting as suppliers the documented agreement can also be a legally binding contract.
Service design life-cycle stage	5 Design and transition of new or changed services	The concepts and activities of the ITIL service life-cycle stages support Clause 5.
Design coordination	5 Design and transition of new or changed services	The ITIL design coordination process provides a single point of coordination and control for all activities and processes within the design stage of the service lifecycle. It can support the whole of Clause 5, particularly 5.1–5.3.
Service level management Service catalogue management	6.1 Service level management	The ITIL service level management process directly supports 6.1. The ITIL service catalogue management process can support 6.1, which contains requirements to agree the service catalogue with the customer and to maintain it.

ITIL process	Part 1 Clause	Comments
		NOTE The support by ITIL for processes such as SLM and business relationship management is complicated by Part 1 not including any requirements for a service portfolio or the service portfolio management process. The more strategic approach of 7.1 can be seen as being supported by service portfolio management, as described in Chapter 3.
Availability management IT service continuity management	6.3 Service continuity and availability management	The ITIL availability management and service continuity management processes can support 6.3. The requirements for the management of service continuity and availability are combined in the standard but could be implemented separately.
Capacity management Demand management	6.5 Capacity management	The ITIL capacity management process can support 6.5. The ITIL capacity management plan covers both current and forecast demand, supporting 6.5.
Information security management	6.6 Information security management	The ITIL information security management process can support 6.6. There is strong alignment between ITIL and the ISO/IEC 27000 series of International Standards, listed in Appendix G.
3. Service transition book		
Service asset and configuration management	4.1 Management responsibility 5 Design and transition of new or changed services 6.4 Budgeting and accounting for services	The ITIL service asset and configuration management process includes the management of service assets, the integrity of services and service components and maintenance of the CMS that incorporates the CMDB. It supports Clause 5, 9.1, 9.2 and 9.3. Part 1 also covers the management of assets in 4.1, 6.4 and 6.6.2. ITIL also provides support for designing and documenting the

ITIL process	Part 1 Clause	Comments
	6.6.2 Information security controls 9.1 Configuration management 9.2 Change management 9.3 Release and deployment management	interface to financial asset management, which is also required by 6.4.
Knowledge management	4.3 Documentation management 9.3 Configuration management	The ITIL knowledge management process includes management of documentation (in Part 1, documents and records). The ITIL service knowledge management system includes advice on a CMDB and can support 9.1. This clause also has requirements for an interface to other processes, for information on changes to CIs relevant to other processes, for example, the resolution and control processes.
Change management	4.5 Establish and improve the SMS 5 Design and transition of new or changed services 9.2 Change management	The ITIL change management process can be used to support 9.2. It can also support other clauses in Part 1, including Clauses 4.5 and 5. There are many references in Part 1 to the use of change management for managing changes to the SMS and services so the ITIL advice is broadly relevant to many Part 1 clauses.
Change evaluation	5 Design and transition of new or changed services 9.2 Change management 9.3 Release and deployment management	The ITIL evaluation process covers the evaluation of a change and it can support Clauses 5, 9.2 and 9.3 of the standard.

ITIL process	Part 1 Clause	Comments
Service transition life-cycle stage	5 Design and transition of new or changed services	The concepts and activities of the ITIL service life-cycle stages support Clause 5.
Transition planning and support	5 Design and transition of new or changed services	ITIL transition planning and support process includes the overall planning for service transitions and coordination of the required resources. It supports the whole of Clause 5.
Release and deployment management	5.4 Transition of new or changed services 9.3 Release and deployment management	The ITIL release and deployment management process can be used directly to support 9.3. As Clause 5 requires all changes managed under Clause 5 to be also managed via release and deployment management, ITIL also supports this activity.
Service validation and testing	5.4 Transition of new or changed services 9.3 Release and deployment management	The ITIL release and deployment process uses service validation and testing and it supports 5.4 and 9.3.
4. Service operation book		
Operational activities of processes covered in other life-cycle stages	4 Service management system general requirements 4.3 Documentation management 4.5 Establish and improve the SMS 6.1 Service level management	The ITIL knowledge management activities include gathering, storing and assessing all the data and information required for service management that is held in the logical Service knowledge management systems (SKMS). These activities support 4.3. In ITIL IT operations covers IT operations management including aspects of technology management, facilities and data centre management to support 4.5.3. The operational activities for monitoring and control support 4.5. The improvement of operational activities supports 4.5.3 to 4.5.5.

ITIL process	Part 1 Clause	Comments
	6.3 Service continuity and availability management 6.4 Budgeting and accounting 6.5 Capacity management 6.6 Information security management 9.1 Configuration management 9.2 Change management 9.3 Release and deployment management	The ITIL demand management and capacity management activities supports Clauses 4, 6.5 and 7.1. The ITIL service level management operational activities support 6.1 The ITIL availability management and IT service continuity management activities support 6.3, including testing and execution of the service continuity and availability plans. The ITIL budgeting and accounting activities support 6.4. For example, operational managers review expenditure against budget and take action. The ITIL information security management operational activities and controls support Clause 6.6 to protect against breaches to security measures. The ITIL service asset and configuration management operational activities support 9.1, 9.2 and 9.3 including updates to the CMDB. The ITIL change management operational activities support 9.1. The ITIL release and deployment management activities support 9.3.
Event management	4.5.3 Implement and operate the SMS (Do) 4.5.4 Monitor and review the SMS (Check) 6.3 Service continuity and availability management 6.5 Capacity management	No direct mapping from ITIL to the standard. However, 4.5.3 includes monitoring and reporting on the performance of service management activities 4.5.4 includes suitable methods for monitoring and measuring the SMS and the services. 6.3 and 6.5 include monitoring of services and taking action as required. Monitoring and control activities in ITIL are supported by event management, which can be used to support these clauses. An event

ITIL process	Part 1 Clause	Comments
		is only specifically covered in the standard if it becomes an incident, service request, problem or change.
Access management	6.3 Service continuity and availability management 6.6 Information security management 8.1 Incident and service request management	There is no direct mapping between ITIL and a clause in Part 1. In ITIL the access management process covers the operational activities to execute the information security controls and requirements in 6.6, e.g. the development of suitable controls for access, including access to services or information by external organizations. As 6.3 includes requirements for access rights in the event of a major loss of service, support is also provided by ITIL. Support for 8.1 is also provided, as access requests can be classed as a service request.
Incident management Request fulfilment	8.1 Incident and service request management	The ITIL incident management and request fulfilment processes can be used to support 8.1. The management of incidents and service requests is combined into one process in the standard but could be implemented separately.
Problem management	8.2 Problem management	The ITIL problem management process can be used to support 8.2.
5. Continual service improvement book		
7-step improvement process	4.5 Establish and improve the SMS 4.5.4 Monitor and review the SMS (Check) 4.5.5 Maintain and improve the SMS (Act)	Measurements are a common theme for both ITIL and the ISO/IEC 20000 series. ITIL provides guidance to support many requirements in Part 1. This includes planning and setting up the SMS, implementation and operation of the SMS, communications, including via service reporting and as input to continual improvement cycles. Support by ITIL is particularly important for 4.5,

ITIL process	Part 1 Clause	Comments
	6.2 Service reporting	designing, setting up, operating and improving the SMS and services. The broad-based advice on monitoring and measuring can also support the 6.2 service reporting process.
7-step improvement process	4.1.2 Service management policy 4.5 Establish and improve the SMS	The ITIL 7-step improvement process is strongly aligned to the Plan-Do-Check-Act cycle in 4.5. The importance of top management commitment to the Plan-Do-Check-Act cycle is also supported by the ITIL improvement strategy, as part of setting the strategy for service management.
7-step improvement process	6.2 Service reporting	The ITIL 7-step improvement process can support 6.2. It defines what to measure, gathering the data, processing the data, analysing the data, presenting and using the information.

Appendix G Bibliography and other sources of information

Standards

The standards publications are listed in numerical order.

ISO 9000:2005, *Quality management systems — Fundamentals and vocabulary*

ISO 9001:2008, *Quality management systems — Requirements*

ISO 9004:2009, *Managing for the sustained success of an organization — A quality management approach*

ISO 9241-11: 1999, *Ergonomic requirements for office work with visual display terminals (VDTs) — Guidance on usability*

ISO 9241-210:2010, *Ergonomics of human-system interaction — Human-centred design for interactive systems*

ISO 9241-151:2008, *Ergonomics of human-system interaction — Guidance on World Wide Web user interfaces*

ISO 10002:2004, *Quality management — Customer satisfaction — Guidelines for complaints handling in organizations*

ISO 10007:2003, *Quality management systems — Guidelines for configuration management*

ISO/IEC 15288, (draft for public comment), *Systems and software engineering — System life cycle processes*

ISO/IEC 15504-1:2004, *Information technology — Process assessment — Part 1: Concepts and vocabulary*

ISO/IEC 15504-2:2003, *Software engineering — Process assessment — Part 2: Performing an assessment*

ISO/IEC 15504-3:2004, *Information technology — Process assessment — Part 3: Guidance on performing an assessment*

ISO 19011:2002, *Guidelines for quality and/or environmental management systems auditing*

ISO/IEC 19770-1:2006, *Information technology — Software asset management — Part 1: Processes*

ISO/IEC 20000-1:2011, *Information technology — Service management — Part 1: Service management system requirements*

ISO/IEC 20000-2:2005, *Information technology — Service management — Part 2: Code of practice* [to be replaced in late 2011]

PD ISO/IEC TR 20000-3:2009, *Information technology — Service management — Part 3: Guidance on scope definition and applicability of ISO/IEC 20000-1*

PD ISO/IEC TR 20000-4:2010, *Information technology — Service management — Part 4: Process reference model*

PD ISO/IEC TR 20000-5:2010, *Information technology — Service management — Part 5: Exemplar implementation plan for ISO/IEC 20000-1*

ISO/IEC/IEEE 24765:2010, *Systems and software engineering — Vocabulary*

ISO/IEC 27000:2009, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

ISO/IEC 27001:2005, *Information technology — Security techniques — Information security management systems — Requirements*

ISO/IEC 27005:2011, *Information technology — Security techniques — Information security risk management*

ISO 31000:2009, *Risk management — Principles and guidelines*

ISO/IEC 38500:2008, *Corporate governance of information technology*

Other publications

Lynda Cooper, A Guide to the New ISO/IEC 20000-1: The differences between 2005 and 2011 editions, BSI (2011), ISBN-13: 978 0 580 72850 1

Jenny Dugmore, Shirley Lacy, *Introduction to the ISO/IEC 20000 series: IT Service Management,* BSI (2011), ISBN-13: 978 0 580 72846 4

Office of Government Commerce, *Managing Successful Projects with PRINCE2,* TSO (2010), ISBN-13: 978 0113309467

A Guide to the Project Management Body of Knowledge (PMBOK® Guide), 4th edition, Project Management Institute (2010), ISBN: 193069945X, ISBN-13: 978-1930699458

ITIL publications

Cabinet Office, *ITIL Glossaries,* (http://www.best-management-practice.com/IT-Service-Management-ITIL/, (2011)

Cabinet Office, *Service Strategy*, TSO (2011), ISBN-13: 978-0113313075

Cabinet Office, *Service Design*, TSO (2011), ISBN-13: 978-0113313051

Cabinet Office, *Service Transition*, TSO (2011), ISBN-13: 978-0113313068

Cabinet Office, *Service Operation*, TSO (2011), ISBN-13: 978-0113313075

Cabinet Office, *Continual Service Improvement,* TSO (2011), ISBN-13: 978-0113313082

Office of Government Commerce, *The Introduction to the ITIL Service Lifecycle*, TSO (2010), ISBN-13: 978-0113310623

COBIT, ISACA and ITGI Publications

CobiT® 4.1, *The CobiT Framework* [4], www.isaca.org/cobit (2007)

CobiT® User Guide for Service Managers, IT Governance Institute, (2009), ISBN-13:978-1604200713

Implementing and Continually Improving IT Governance, ISACA, (2009), ISBN-13: 978-1604201192

ITGI Enables ISO/IEC 38500:2008 Adoption, IT Governance Institute (2009)

Web addresses

www.iso.org

www.itil-officialsite.com

www.isaca.org

www.itgi.org

[4] The CobiT framework is being updated to COBIT 5.

If you found this book useful, you may also want to buy:

IT Service Management for Small IT Teams
Adam Poppleton and Ken Holmes

Using ISO/IEC 20000 as a guide, this book will direct the reader in a concise way as to the important areas of the standard from which an SME /Small IT unit will gain most benefit. It will provide a straightforward, easy to follow route map to gaining a 'wide and thin' approach to ITSM, making the most of limited resources, so that its benefits are effective in a short timeframe. The ITIL volumes and other guidance, as well as the standard are quite lengthy to read, whereas this book aims to be a short to read and quick to implement guide. The text will be supported by examples and vignettes of 'real world' problems and scenarios, to support the user.

A5 paperback · ISBN 978 0 580 74254 5 · 130pp · £35.00
BSI order reference BIP 0129
For more details see http://shop.bsigroup.com/ISO20000SmallTeams

Introduction to the ISO/IEC 20000 series: IT Service Management
Jenny Dugmore and Shirley Lacy

The book forms the definitive guide to the second edition of ISO/IEC 20000-1. 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 the standard. The book includes a road map to the second edition and how it fits in the bigger picture for best practices.

A5 paperback · ISBN 978 0 580 72846 4 · 236pp · £48.00
BSI order reference BIP 0125
For more details see http://shop.bsigroup.com/ISO20000Introduction

Guide to the new ISO/IEC 20000-1: The differences between the 2005 and 2011 editions
Lynda Cooper

The new edition of ISO/IEC 20000-1 is substantially changed from the original edition published in 2005. The changes will impact any organizations which are already certified to this standard, those who are working towards certification. It will also impact those who use the standard as guidance as well as auditors, trainers and consultants who use the standard for their customers. This book explains why the changes have been made, what the changes are and how to move to the latest edition. It also covers the relationship of the standard to other standards.

A4 Paperback · ISBN 978 0 580 72850 1· 120pp · £36.00
BSI order reference BIP 0124
For more details see http://shop.bsigroup.com/ISO20000DifferencesGuide

A Manager's Guide to Service Management

Jenny Dugmore and Shirley Lacy

This book meets the need for a generic, broadly based book on service management. It provides an introduction on how service management best practices and standards can help a service provider to deliver services that add value for customers at the right cost and risk. It describes service management concepts and the broader service management landscape. This 6th edition is substantially re-focused to give a broader based picture of the most important service management best practices, how they relate and how they can (or cannot) be used together.

Jenny Dugmore works for Service Matters as a service management consultant. Jenny also has a background in operational line management. She is chair of the ISO group responsible for the 20000 series and is co-editor for both the ISO Guidance on the integrated implementation of ISO/IEC 20000 and ISO/IEC 27001 and the second edition of ISO/IEC 20000-3. She is involved in certification schemes and examination boards for ISO/IEC 20000 and 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, specializing in the application of service management best practices to deliver service excellence and 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 ITIL Service Transition publication and project mentor for the ITIL 2011 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 group that develop IT service management and process assessment standards and the new ISO/IEC 33000 series.

'Service management is best expressed in terms of the relationships of multiple best practices, with each practice strength at the forefront of addressing particular performance and service improvements. This is an excellent book for a management understanding of the synergies between ITIL, ISO/IEC 20000 and CoBiT for service management'.
Anthony Orr, Director in CTO office, BMC Software, Inc.

'Shirley and Jenny have produced a readable and practical book on SM that gives the reader an excellent understanding of service management and how it is linked to best practices (ITIL, COBIT and ISO/IEC 20000). It is an essential read for any professional in the service management industry who needs to get to grips with planning, implementing and supporting a successful service management. I thoroughly recommend it'.
Kim Hamilton, Independent Project Manager

BSI order ref: BIP 0005

BSI Group Headquarters
389 Chiswick High Road
London W4 4AL

www.bsigroup.com

The British Standards Institution
is incorporated by Royal Charter

ISBN 978-0-580-72845-7

9 780580 728457