

FOREWORD

As an education and training organization within the IT Service Management (ITSM) industry, we have been impressed by the positive changes introduced by the ITIL® 2011 edition of the ITIL® framework. The evolution of the core processes and concepts provided by the framework provides the more holistic guidance needed for an industry that continues to mature and develop at a rapid pace. We recognize, however, that many organizations and individuals who have previously struggled with their adoption of the framework will continue to find challenges in implementing ITIL® as part of their approach for governance of IT Service Management practices. In light of this, one of our primary goals is to provide the quality education and support materials needed to enable the understanding and application of the ITIL® framework in a wide-range of contexts.

This comprehensive book is designed to complement the in-depth accredited eLearning ITIL® Foundation Certificate in IT Service Management program provided by The Art of Service. The interactive eLearning program uses a combination of narrated presentations with flat text supplements and multiple choice assessments. This book provides added value to the eLearning program by providing additional text and real life examples to further cement your knowledge. Your learning and understanding will be maximized by combining these two study resources, which will ultimately prepare you for the APMG ITIL® Foundation Certificate in IT Service Management exam. This fourth edition also includes appropriate alterations based on the recent review of the framework and the ITIL® 2011 edition Foundation syllabus and associated exams. We have also used student feedback to include improvements to the format and material, including additional content and sample exam questions.

We hope you find this book to be a useful tool in your educational library and wish you every success in your IT Service Management career!

Notice of Rights	All rights reserved. No part of this book may be reproduced or transmitted in any form by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior written permission of the publisher.
Notice of Liability	The information in this book is distributed on an "As Is" basis without warranty. While every precaution has been taken in the preparation of the book, neither the author nor the publisher shall have any liability to any person or entity with respect to any loss or damage caused or alleged to be caused directly or indirectly by the instructions contained in this book or by the products described in it.
Trademarks	Many of the designations used by manufacturers and sellers to distinguish their products are claimed as trademarks. Where those designations appear in this book, and the publisher was aware of a trademark claim, the designations appear as requested by the owner of the trademark. All other product names and services identified throughout this book are used in editorial fashion only and for the benefit of such companies with no intention of infringement of the trademark. No such use, or the use of any trade name, is intended to convey endorsement or other affiliation with this book.

Write a review to receive any free eBook from our Catalog—\$99 Value!

If you recently bought this book, we would love to hear from you! Benefit from receiving a free eBook from our catalog at <http://www.emereo.org/> by writing a review on Amazon (or the online store where you purchased this book) about your last purchase! As part of our continual service improvement process, we love to hear real student experiences and feedback.

How does it work?

To post a review on Amazon, just log in to your account and click on the Create Your Own Review button (under Customer Reviews) of the relevant product page. You can find examples of product reviews in Amazon. If you purchased from another online store, simply follow their procedures.

What happens when I submit my review?

Once you have submitted your review, send us an email at review@emereo.org with the link to your review and the eBook you would like as our thank you from <http://www.emereo.org/>. Pick any book you like from the catalog, up to \$99 RRP. You will receive an email with your eBook as a download link. It's that simple!

HOW TO ACCESS THE eLEARNING PROGRAM

- Direct your browser to: www.theartofservice.org
- Click 'login' (found at the top right of the page)
- Click 'Create New Account'
- Follow the instructions to create a new account. You will need a valid email address to confirm your account creation. If you do not receive the confirmation email, check that it has not been automatically moved to a Junk Mail or Spam folder.
- Once your account has been confirmed, email your User-ID for your new account to key11@theartofservice.com
- You will receive a return email with an enrolment key that you will need to use in order to access the eLearning program. Next time you log in to the site, access the program titled: *ITIL® 2011 Foundation eLearning Program*

Minimum system requirements for accessing the eLearning Program:

Processor	Pentium 4 (1 GHz) or higher
RAM	256MB (512 MB recommended)
OS	Windows XP, Vista, 7, MCE, Mac OSX
Browser	Mozilla Firefox 3+ (recommended), Internet Explorer 6.x or higher, Safari, Opera, Chrome, all with cookies and JavaScript enabled
Plug-Ins	Adobe Flash Player 8 or higher
Internet Connection	Due to multimedia content of the site, a minimum connection speed of 512kbs is recommended. If you are behind a firewall and are facing problems in accessing the course or the learning portal, please contact your network administrator for help.

If you are experiencing difficulties with the Flash Presentations within the eLearning Programs, please make sure that:

1. You have the latest version of Flash Player installed, by visiting
<http://get.adobe.com/flashplayer/>
2. You check that your security settings in your web browser do not prevent these flash modules from playing
3. For users of Internet Explorer 7, a solution involves DESELECTING "Allow active content to run files on my computer" in Internet Explorer -->Tools, Options, Advanced, Security settings.

CONTENTS

<u>FOREWORD</u>	1
<u>HOW TO ACCESS THE eLEARNING PROGRAM</u>	4
<u>INTRODUCTION</u>	11
Benefits of ITSM	12
Business and IT Alignment	13
What is ITIL®?	15
<u>COMMON TERMINOLOGY</u>	18
What are Services?	20
Processes and Functions	22
<u>THE SERVICE LIFECYCLE</u>	29
Mapping the Concepts of ITIL® to the Service Lifecycle.....	30
How does the Service Lifecycle work?.....	32
<u>SERVICE STRATEGY</u>	34
Purpose of Service Strategy	35
Benefits of Service Strategy	36
Major Concepts.....	37
Service Strategy Processes.....	43

Service Strategy Review Questions.....	65
<hr/>	
SERVICE DESIGN	68
Purpose and Value.....	68
The Four Perspectives (Attributes) of ITSM.....	70
Major Concepts.....	71
Service Design Processes	73
Service Design Summary.....	144
Service Design Scenario.....	145
Service Design Review Questions	147
Service Transition	150
Purpose	151
Value	152
Service Transition Processes.....	153
Service Transition Summary	191
Service Transition Scenario	192
Service Transition Review Questions.....	193
<hr/>	
SERVICE OPERATION	196
Purpose	196
Value to the business.....	197

Major Concepts.....	198
Service Operation Functions	199
Service Operation Processes	217
Service Operation Summary	258
Service Operation Scenario.....	259
Service Operation Review Questions	260
<hr/> CONTINUAL SERVICE IMPROVEMENT	264
Purpose	264
Scope.....	265
Value to the Business.....	267
Major Concepts.....	268
Seven-Step Improvement Process	276
Continual Service Improvement Scenario	281
Continual Service Improvement Review Questions.....	282
<hr/> ITIL® FOUNDATION EXAM TIPS	284
<hr/> ANSWERS FOR REVIEW QUESTIONS	285
Service Strategy.....	285
Service Design	288
Service Transition	291
Service Operation	294

Continual Service Improvement	298
<hr/>	
GLOSSARY	300
<hr/>	
ABBREVIATIONS	328
<hr/>	
CERTIFICATION	330
<hr/>	
ITIL® Certification Pathways	330
<hr/>	
ISO/IEC 20000 Pathways.....	331
<hr/>	
INDEX	332

INTRODUCTION

Looking back on a period where corporate giants fell and government bailouts were measured in the billions, not to mention the overwhelming natural disasters that have occurred all over the world, the challenges faced by a typical IT Service Provider may seem of low priority. But now that IT budgets have come under more financial scrutiny than ever before, the value provided by managing IT with controlled, repeatable, and measurable processes has become all the more obvious. So, for the modern Chief Information Officer (CIO), employing quality IT Service Management (ITSM) practices can often help in achieving a quality sleep each night.

The term IT Service Management is used in many ways by different management frameworks and the organizations that seek to use them. While there are variations across these different sources of guidance, common elements for defining ITSM include:

- Description of the **processes** required to deliver and support IT Services for customers
- A focus on delivering and supporting the **technology or products** needed by the business to meet key organizational objectives or goals
- Definition of roles and responsibilities for the **people** involved, including IT staff, customers, and other stakeholders
- The management of **external suppliers (partners)** involved in the delivery and support of the technology and products being delivered and supported by IT

The combination of these elements provide the capabilities required for an IT organization to deliver and support quality IT Services that meet specific business needs and requirements.

The official ITIL® definition of IT Service Management is found within the Service Design volume (page 16), and defines ITSM as "The implementation and management

of quality IT services that meet the needs of the business. IT service management is performed by IT service providers through an appropriate mix of people, process and information technology". Organizational capabilities are influenced by the needs and requirements of customers, the culture that exists within the service organization, and the intangible nature of the output and intermediate products of IT services.

However, IT Service Management comprises more than just these capabilities alone, being complemented by an industry of professional practice and wealth of knowledge, experience, and skills. The ITIL® framework has developed as a major source of good practice in Service Management and is used by organizations worldwide to establish and improve their ITSM practices.

Benefits of ITSM

WHILE THE BENEFITS OF APPLYING IT Service Management practices vary depending on the organization's needs, some typical benefits include:

- Improved quality service provision
- Cost-justifiable service quality
- Design of services that meet business, customer, and user demands
- Integrated and centralized processes
- Transparency of the roles and responsibilities for service provision
- Continual improvement, incorporating lessons learnt into future endeavors
- Measurable quality, performance, and efficiency attributes

It is also important to consider the range of stakeholders who can benefit from improved ITSM practices. As perspectives will differ for each stakeholder, the benefits provided by enhanced ITSM practices may apply to one or more of the following parties:

- Senior management
- Business unit managers
- Customers
- End users
- IT staff
- Suppliers
- Shareholders

Business and IT Alignment

A COMMON THEME IN ANY IT Service Management framework is to enable and demonstrate business and IT alignment. When staff members of an IT organization have only an internal focus on the technology being delivered and supported, they lose sight of the actual purpose and benefit that their efforts deliver to the business and customers. A way in which to communicate how IT supports the business is using Figure 1.A (on page 14), which demonstrates business and IT alignment.

Figure 1.A divides an organization into a number of supporting layers that work towards meeting a number of organizational goals. These layers are communicated by the following:

Organization	What are the key strategic goals and objectives for the organization? These objectives define who we are as an organization and where we want to be in the future.
CORE Business Processes	These are represented by the repeatable business activities that produce desirable results for the business. Without these results, the organizational objectives defined above would not be supported or achieved.
IT Service Organization	Defines the IT Services and supporting infrastructure that is required to enable the effective and efficient execution of the business processes above. IT Services are used by the business to facilitate and enhance outcomes, including improved efficiency of operations or ensuring accuracy in the records and information being managed.
IT Service Management	Made up by the repeatable, managed, and controlled processes used by the IT department that enable quality and efficiency in the delivery and support of the IT Services above.
IT Technical Activities	The actual technical activities required as part of the execution of the ITSM processes above. ITSM is utilized to ensure that any resources and effort spent performing the technical activities are optimized according to the greatest business need or reward. As these activities are technology specific (e.g., configuring application server), they will not be a focus of this book's content.

Each layer within this structure is utilized to support the layer(s) above. At the same time, each layer will in some way influence the layer below it. For example, a business process that is required to be executed at all times without disruptions (e.g., emergency health services) would result in highly resilient IT services being implemented, supported by ITSM processes that reduce the risk and impact of disruptions occurring.

OUR BUSINESS: A FASHION STORE

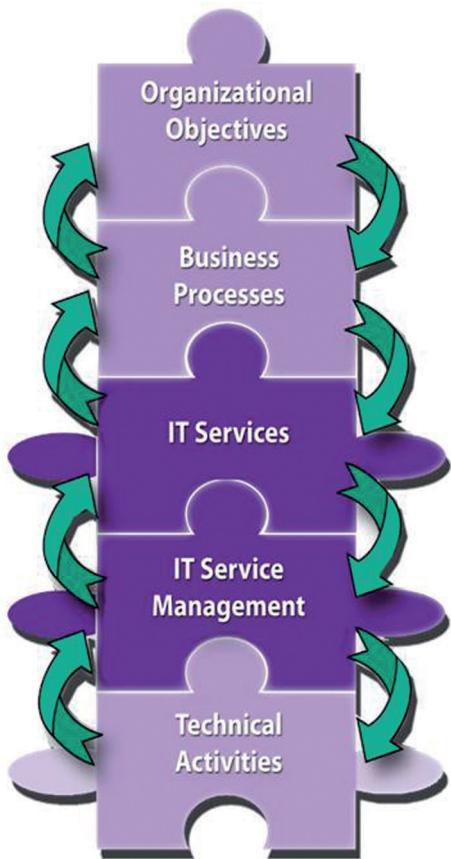


Figure 1.A—Business and IT Alignment

- Management, Capacity Management etc.)
- Available when we need it (Availability Management, Incident Management etc.)
- Provisioned cost-effectively (Financial Management, Service Level Management)

If we don't manage the IT Services appropriately, we cannot rely on these services to be available when we need them. If too many disruptions occur, we cannot adequately support our business processes effectively and efficiently. If

What are some of our organization's objectives or strategic goals?

- We want to increase profits by 15 percent each year
- We want to have a good image and reputation with a loyal customer base

What Business Processes aid in achieving those objectives?

- Retail/sales
- Marketing
- Manufacturing
- Procurement, HR, finance etc.

What IT Services are these business processes dependent on?

- Websites (internal and external)
- Communication services (email, video conferencing)
- Automatic procurement system for buying products
- Point of Sale Services

We have ITSM in order to make sure that IT Services are:

- What we need (Service Level

the business processes are not operating as they should, we will ultimately fail to support and achieve our overall organization's objectives!

Also note the relationship between IT Service Management processes and the technical activities below. Used properly, ITSM processes can optimize the time, effort, and other resources spent performing technical activities, ensuring that all staff actions are working in accordance to agreed business priorities and objectives.

This is just a simple example used to illustrate the relationship between ITSM and the organization. Any approach used to improve ITSM practices should always be carefully considered to ensure that the plans suit the organization in terms of:

- Size (number of staff, customers, IT devices etc.)
- Geographical dispersion
- Culture and ethos
- Current maturity and capability levels

What is ITIL®?

ITIL® STANDS FOR THE INFORMATION Technology Infrastructure Library. ITIL® is the international de facto management framework describing best practices for IT Service Management. The ITIL® framework evolved from the UK government's efforts during the 1980s to document how successful organizations approached service management. By the early 1990s, they had produced a large collection of books documenting the best practices for IT Service Management. This library was eventually entitled the IT Infrastructure Library. The Office of Government Commerce in the UK continues to operate as the trademark owner of ITIL®.

ITIL® has gone through several evolutions and was most recently refreshed and reviewed with the release of the 2011 edition. Through these evolutions, the scope of practices documented has increased in order to stay current with the continued maturity of the IT industry and meet the needs and requirements of the ITSM professional community.

ITIL® is only *one of many* sources for ITSM best practices and should be used to complement any other set of practices being used by an organization.

Five volumes make up the ITIL® 2011 Edition:

- Service Strategy
- Service Design
- Service Transition
- Service Operation
- Continual Service Improvement

Each volume provides the guidance necessary for an integrated approach and addresses capabilities' direct impact on a service provider's performance. The structure of the ITIL® framework is that of the service lifecycle. It ensures organizations are able to leverage capabilities in one area for learning and improvements in others. The framework is used to provide structure, stability, and strength to service management capabilities with durable principles, methods, and tools. This enables service providers to protect investments and provide the necessary basis for measurement, learning, and improvement.

In addition to the core publications, there is also *ITIL® Complementary Guidance*. This consists of a complementary set of publications with guidance specific to industry sectors, organization types, operating models, and technology architectures. At present, this complementary guidance is available by subscription from <http://www.bestpracticelive.com>.

Best practices

IGNORING PUBLIC FRAMEWORKS AND STANDARDS can needlessly place an organization at a disadvantage. Organizations should seek to cultivate their own proprietary knowledge on top of a body of knowledge developed from using public frameworks and standards.

Public frameworks (ITIL®, COBIT, CMMI etc.): Frameworks are scaled and adapted by the organization when implemented, rather than following a prescriptive set of practices (standards). Examples of public frameworks for ITSM include:

- ITIL®
- COBIT—The Control Objectives for Information and related Technology
- Capability Maturity Model Integrated (CMMI) for IT Services

Standards: Usually a formal document that establishes uniform engineering or technical criteria, methods, processes, and practices. Unlike frameworks, they are prescriptive in declaring mandatory elements that must be demonstrated. Examples of standards relating to ITSM are:

- ISO/IEC 20000—International Standard for IT Service Management
- ISO/IEC 27001—International Standard for Information Security Management Systems
- ISO/IEC 38500—Corporate governance of information technology standard

Proprietary knowledge of organizations and individuals: Specific expertise developed for internal purposes or developed in order to sell to other organizations (e.g., Gartner).

Generally, best practices are defined as those formalized as a result of being **successful in wide-industry use.**

COMMON TERMINOLOGY

Critical to our ability to participate with and apply the concepts from the ITIL® framework is the need to be able to speak a common language with other IT staff, customers, end-users, and other involved stakeholders. This chapter documents the important common terminology that is used throughout the ITIL® framework.

Care should be taken when attempting the ITIL® Foundation exam, as there will be a number of questions that seek to ensure the candidate has an effective grasp of the terminology used throughout the framework.

A full glossary has been included at the back of this book for terminology and acronyms that are covered under the ITIL® 2011 Foundation syllabus. The following introductory glossary is provided as an introduction to the common terms found within the framework. Throughout the book, relevant terms will be discussed in more detail in the context of their corresponding process or lifecycle stages.

Terminology	Explanations
Baselines	<p>(<i>ITIL® Continual Service Improvement</i>) (<i>ITIL® Service Transition</i>) A snapshot that is used as a reference point. Many snapshots may be taken and recorded over time but only some will be used as baselines. For example:</p> <ul style="list-style-type: none"> • An ITSM baseline can be used as a starting point to measure the effect of a service improvement plan • A performance baseline can be used to measure changes in performance over the lifetime of an IT service • A configuration baseline can be used as part of a back-out plan to enable the IT infrastructure to be restored to a known configuration if a change or release fails
Business Case	<p>A decision support and planning tool that projects the likely consequences of a business action. It provides justification for a significant item of expenditure. Includes information about costs, benefits, options, issues, risks, and possible problems.</p>
Capabilities	<p>The ability of an organization, person, process, application, CI, or IT service to carry out an activity. Capabilities can be described as the functions and processes utilized to manage services. These are intangible assets of an organization that cannot be purchased but must be developed and matured over time. The ITSM set of organizational capabilities aims to enable the effective and efficient delivery of services to customers.</p>
External Service Providers	<p>Service provider that provides IT services to external customers, e.g., providing internet hosting solutions for multiple customers.</p>
Functions	<p>A team or group of <i>people</i> and the tools they use to carry out one or more processes or activities. Functions provide units of organization responsible for specific outcomes. <i>ITIL® Functions covered include:</i></p> <ul style="list-style-type: none"> • Service Desk • Technical Management • Application Management • IT Operations Management
Internal Service Providers	<p>An internal service provider that is embedded within a business unit, e.g., one IT organization within each of the business units. The key factor is that the <i>IT services provide a source of competitive advantage</i> in the market space the business exists in.</p>
IT Service Management	<p>A set of specialized organizational capabilities for providing value to customers in the form of services.</p>

Terminology	Explanations
Process	<p>A set of <i>coordinated activities</i> combining and implementing resources and capabilities in order to produce an outcome and provide value to customers or stakeholders.</p>
	<p>Processes are <i>strategic assets</i> when they create competitive advantage and market differentiation. They <i>may</i> define roles, responsibilities, tools, management controls, policies, standards, guidelines, activities, and work instructions if they are needed.</p>
Process Owner	<p>The person/role responsible for ensuring that the process is fit for the desired purpose and is accountable for the outputs of that process.</p>
	<p>Example: The owner for the Availability Management Process</p>
Process Manager	<p>The person/role responsible for the operational management of a process. There may be several managers for the one process. They report to the Process Owner.</p>
Resources	<p>A generic term that includes IT infrastructure, people, money, or anything else that might help to deliver an IT service. Resources are also considered to be tangible assets of an organization.</p>
Service	<p>A means of delivering value to customers by facilitating outcomes customers want to achieve without the ownership of specific costs or risks. The role of the service provider is to manage these costs and risks appropriately, spreading them over multiple customers if possible.</p>
Service Owner	<p>The person/role accountable for the delivery of a specific IT Service. They are responsible for continual improvement and management of change affecting services under their care.</p>
	<p>Example: The owner of the Payroll Service</p>
Shared Service Providers	<p>An internal service provider that provides shared IT service to more than one business unit, e.g., one IT organization to service all businesses in an umbrella organization. IT Services for this provider do not normally provide a source of competitive advantage but, instead, <i>support effective and efficient business processes</i> across an organization.</p>

What are Services?

THE CONCEPT OF IT SERVICES as opposed to *IT components* is central to understanding the Service Lifecycle and IT Service Management principles in general. It requires not just a learned set of skills but also a way of thinking that often challenges the traditional instincts of IT workers to focus on the individual components (typically

the applications or hardware under their care) that make up the IT infrastructure. The mindset requires, instead, an alternative outlook to be maintained, incorporating the end-to-end service perspective for what their organization actually provides to its customers.

The official definition of a service is "a means of delivering value to customers by facilitating outcomes customers want to achieve without the ownership of specific costs or risks". But what does this actually mean? The following analogy explains some of the key concepts in a way that most (food lovers) will understand.

While most people do enjoy cooking, there are often times when they wish to enjoy quality food without the time and effort required to prepare a meal. If they were to cook, they would need to go to a grocery store, buy the ingredients, take these ingredients home, prepare and cook the meal, set the table, and, of course, clean up the kitchen afterwards. The alternative is that they can go to a restaurant that delivers a service that provides them with the same outcome (a nice meal) without the time, effort, and general fuss required if they were to cook it themselves.

Now consider how that person would identify the quality and value of that service being provided. It is not just the quality of the food itself that will influence their perceptions, but also:

- The cleanliness of the restaurant
- The friendliness and customer service skills of the waiters and other staff
- The ambience of the restaurant (lighting, music, decorations etc.)
- The time taken to receive the meal (and was it what they asked for?)
- Did they offer a choice of beverages?

If any one of these factors does not meet the person's expectations, then ultimately the perceived quality and value delivered to them as a customer is negatively impacted. Now, relate this to an IT staff member's role in provisioning an IT Service. If they focus only on the application or hardware elements provided and forget or ignore the importance of the surrounding elements that make up the end-to-end service, just like in the example of the restaurant, the customer experience and perceived quality and value will be negatively impacted.

But if they take a service-oriented perspective, they also ensure that:

- Communication with customers and end users is effectively maintained

- Appropriate resolution times are maintained for end user and customer enquiries
- Transparency and visibility of the IT organization and where money is being spent is maintained
- The IT organization works proactively to identify potential problems that should be rectified or improvement actions that could be made

Using these principles, every phone call to the Service Desk or email request for a password reset presents an opportunity to demonstrate service excellence and a commitment to our customers.

To ensure that a service is managed with a business focus, the definition of a single point of accountability is absolutely essential to provide the level of attention and focus required for its delivery.

The service owner is accountable for the delivery of a specific IT service. The service owner is responsible to the customer for the initiation, transition, and ongoing maintenance and support of a particular service and accountable to the IT director or service management director for the delivery of the service. The service owner's accountability for a specific service within an organization is independent of where the underpinning technology components, processes, or professional capabilities reside.

Service ownership is as critical to service management as establishing ownership for processes that cross multiple vertical silos or departments. It is possible that a single person may fulfill the service owner role for more than one service. The service owner is responsible for continual improvement and the management of change affecting the service under their care. The service owner is a primary stakeholder in all of the underlying IT processes that enable or support the service they own.

Processes and Functions

Defining Processes

PROCESSES CAN BE DEFINED AS a structured set of activities designed to accomplish a specific objective. A process takes one or more defined inputs and turns them into defined outputs.

Processes define actions, dependencies, and sequence. Well-defined processes can improve productivity within and across organizations and functions. Process characteristics include:

- **Measurability:** We are able to measure the process in a relevant manner. It is performance-driven. Managers want to measure cost, quality, and other variables, while practitioners are concerned with duration and productivity.
- **Specific results:** The reason a process exists is to deliver a specific result. This result must be individually identifiable and countable.
- **Customers:** Every process delivers its primary results to a customer or stakeholder. Customers may be internal or external to the organization, but the process must meet their expectations.
- **Responsiveness to specific triggers:** While a process may be ongoing or iterative, it should be traceable to a specific trigger.

The process owner role is accountable for ensuring that a process is fit for purpose. This role is often assigned to the same person who carries out the process manager role, but the two roles may be separate in larger organizations. The process owner role is accountable for ensuring that their process is performed according to the agreed and documented standard and meets the aims of the process definition.

The process manager role is accountable for operational management of a process. There may be several process managers for one process, for example, regional change managers or IT service continuity managers for each data centre. The process manager role is often assigned to the person who carries out the process owner role, but the two roles may be separate in larger organizations.

The process practitioner is responsible for carrying out one or more process activities. In some organizations and for some processes, the process practitioner role may be combined with the process manager role; in other organizations, there may be large numbers of practitioners carrying out different parts of the process.

The process practitioner's responsibilities typically include:

- Carrying out one or more activities of a process
- Understanding how their role contributes to the overall delivery of service and creation of value for the business

- Working with other stakeholders, such as their manager, co-workers, users, and customers, to ensure that their contributions are effective
- Ensuring that inputs, outputs, and interfaces for their activities are correct
- Creating or updating records to show that activities have been carried out correctly

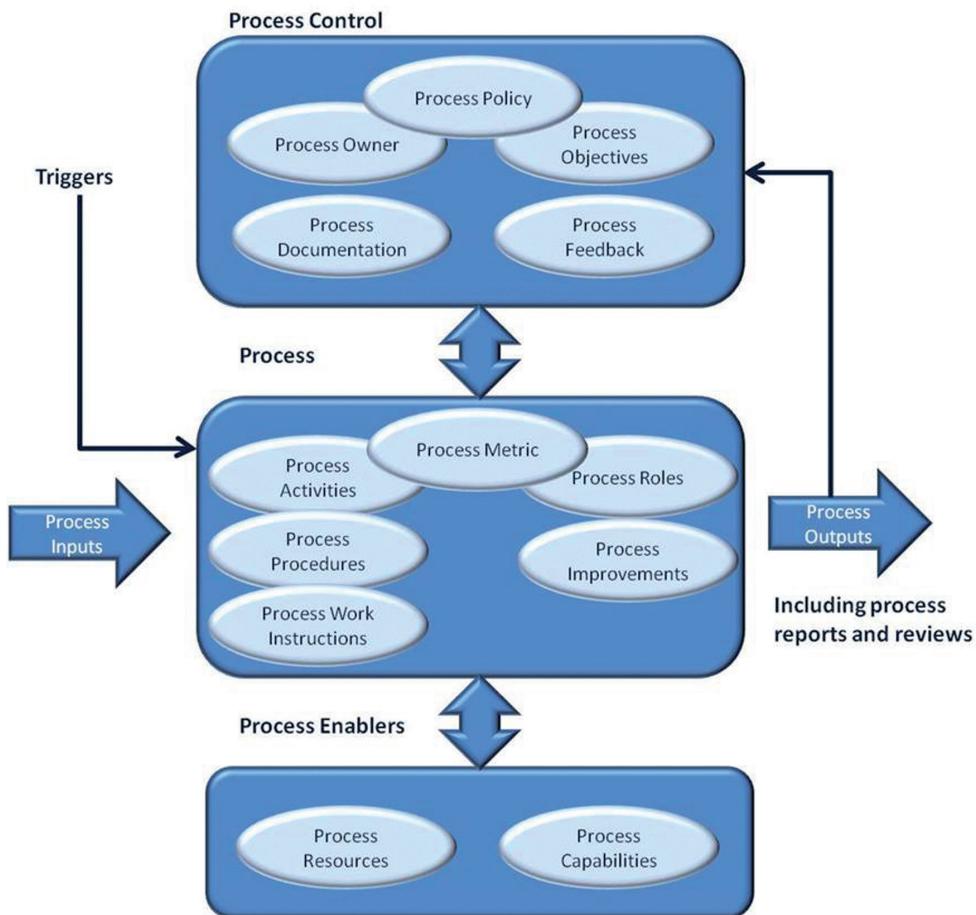


Figure 2.B—Generic Process Elements

© Crown Copyright 2011 Reproduced under license from OGC

THIS PREVIOUS FIGURE DESCRIBES THE physical components of processes, which are tangible and, therefore, typically get the most attention. In addition to the physical components, there are behavioral components, which are for the most part intangible and are part of an underlying pattern so deeply embedded and recurrent that it is displayed by most members of the organization and includes decision-making, communication, and learning processes. Behavioral components have no independent existence that is separate from the work processes in which they appear, but, at the same time, they greatly affect and impact the form, substance, and character of activities and subsequent outputs by shaping how they are carried out.

So when defining and designing processes, it is important to consider both the physical and behavioral aspects that exist. This may be addressed by ensuring the all required stakeholders (e.g., staff members, customers, and users etc.) are appropriately involved in the design of processes so that:

- They can communicate their own ideas, concerns, and opinions that might influence the way in which processes are designed, implemented, and improved. Of particular importance may be current behaviors that have not been previously identified, which may affect the process design and implementation.
- Stakeholder groups are provided adequate training and education regarding how to perform their role within the process and what value the process provides for.
- Stakeholders generally feel empowered in the change being developed, and, therefore, are more likely to respond positively rather than actively or passively resisting the organizational changes occurring.

Defining Functions

FUNCTIONS REFER TO THE LOGICAL grouping of roles and automated measures that execute a defined process, an activity, or combination of both. The functions that will be discussed within the Service Operation stage are needed to manage the steady state operation IT environment. Just like in many sporting activities where each player will have a specific role to play in the overall team strategy, IT functions define the different roles and responsibilities required for the overall design, delivery, and management IT Services.

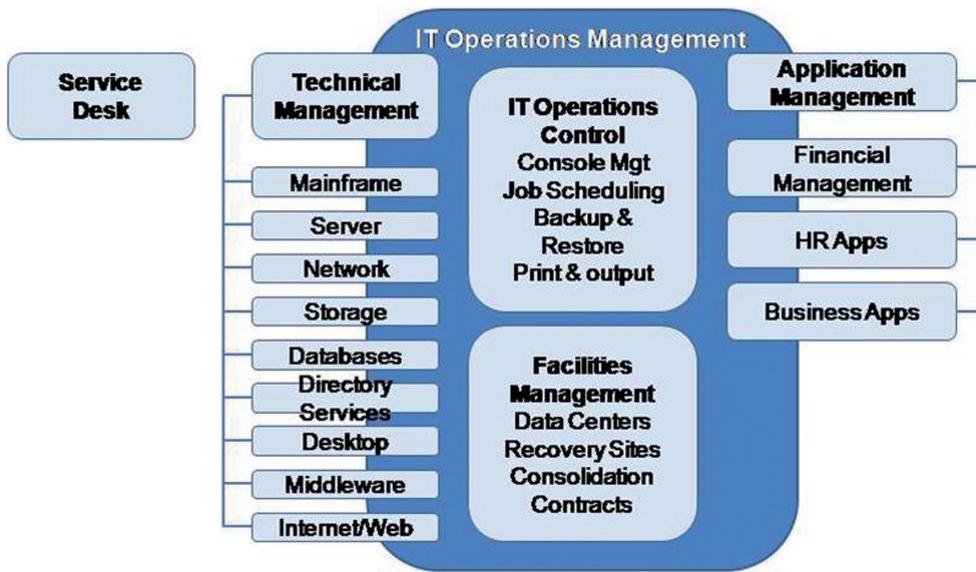


Figure 2.C—The ITIL® Functions from Service Operation

RACI Model

IT IS SAID THAT PROCESSES are perfect ... until people get involved. This saying comes from the perceived failure of processes in many organizations, which can frequently be attributed to misunderstandings of the people involved and a lack of clarity regarding the roles and responsibilities that exist.

A useful tool to address this issue, assisting with the definition of the roles and responsibilities when designing processes, is the RACI Model. RACI stands for:

R—Responsibility (actually does the work for that activity but reports to the function or position that has an "A" against it.)

A—Accountability (is made accountable for ensuring that the action takes place, even if they might not do it themselves. This role implies ownership.)

C—Consult (advice/guidance/information can be gained from this function or position prior to the action taking place.)

I—Inform (the function or position that is told about the event after it has happened.)

	Service Desk	Desktop	Applications	Operations Manager
Logging	RACI			CI
Classification	RACI	RCI		CI
Investigation	ACI	RCI	RCI	CI

Figure 2.D—The RACI Model

A RACI MODEL IS USED to define the roles and responsibilities of various functions in relation to the activities of Incident Management.

General rules that exist:

- Only 1 “A” per row can be defined (ensures accountability, more than one “A” would confuse this)
- At least 1 “R” per row must be defined (shows that actions are taking place) with more than one being appropriate where there is shared responsibility.

In the example RACI model given, the Service Desk is both responsible and accountable for ensuring that incidents are logged and classified, but not responsible for the subsequent investigation, which in this case will be performed by other functional teams.

THE SERVICE LIFECYCLE

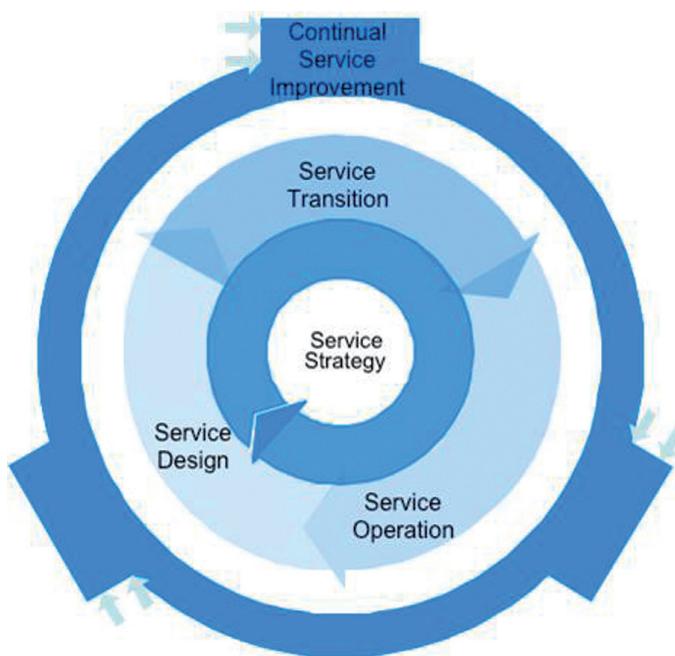


Figure 3.A—ITIL® Service Lifecycle Model

© Crown Copyright 2011 Reproduced under license from OGC

Lifecycle: The natural process of stages that an organism or inanimate object goes through as it matures. For example, the stages that a human goes through are birth, infant, toddler, child, pre-teen, teenager, young adult, adult, elderly adult, and death.

The concept of the *Service Lifecycle* is fundamental to ITIL® 2011. Previously, much of the focus of ITIL® was on the *processes* required to design, deliver, and support services for customers. As a result of this previous focus on processes, Version 2 of the ITIL® Framework provided best practices for ITSM based around the **how** questions.

These included:

- How should we design for availability, capacity, and continuity of services?
- How can we respond to and manage incidents, problems, and known errors?

As ITIL® 2011 now maintains a holistic view covering the entire lifecycle of a service, no longer does ITIL® just answer the how questions, but also **why**?

- Why does a customer need this service?
- Why should the customer purchase services from us?
- Why should we provide (x) levels of availability, capacity, and continuity?

By first asking these questions, it enables a service provider to provide overall **strategic objectives** for the IT organization, which will then be used to direct *how* services are **designed, transitioned, supported, and improved** in order to deliver optimum value to customers and stakeholders.

The ultimate success of service management is indicated by the strength of the relationship between customers and service providers. The 5 stages of the Service Lifecycle provide the necessary guidance to achieve this success. Together they provide a body of knowledge and set of good practices for successful service management.

This end-to-end view of how IT should be integrated with business strategy is at the heart of ITIL's® five core volumes.

Mapping the Concepts of ITIL® to the Service Lifecycle

THERE HAS BEEN MUCH DEBATE as to exactly how many processes exist within ITIL® 2011. Questions asked include:

- What exactly constitutes a process?
- Shouldn't some processes be defined as functions?
- Why has x process been left out of this study material?

In developing this material, we have based our definitions of processes and functions, and where they fit within the lifecycle, on the guidance provided by the ITIL® 2011 Foundation syllabus produced by APMG and the OGC ITIL® 2011 Service

Lifecycle suite of books. Figure 3.B demonstrates the processes and functions of ITIL®, in relation to the five Service Lifecycle stages that are covered at this foundation level.

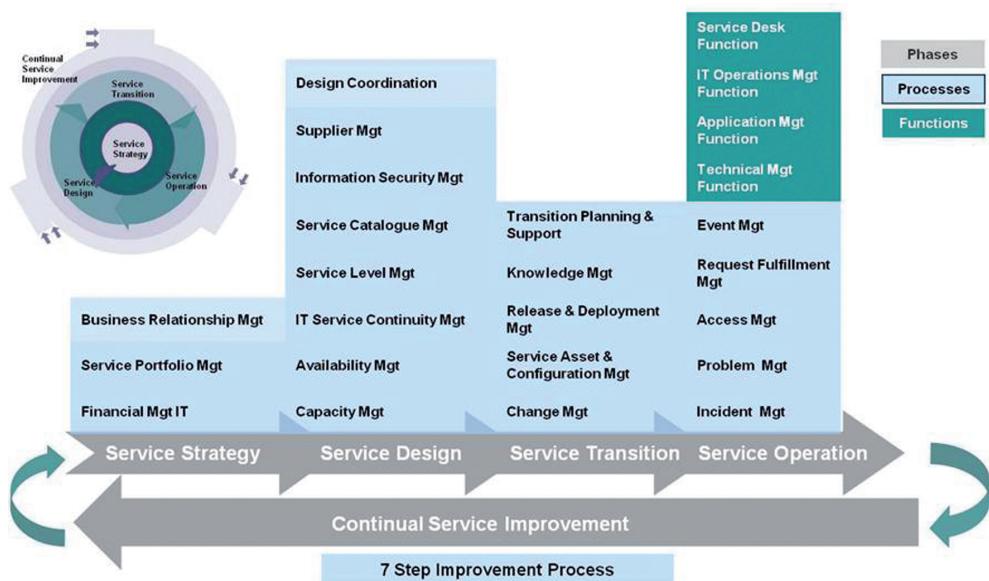


Figure 3.B—The Major Concepts of ITIL® 2011 Foundation Level

Note:

- The Service Lifecycle stages (and ITIL® books) are shown through the arrows at the bottom
- The concepts in light shading are the ITIL® 2011 processes covered within the foundation program
- The concepts in dark shading are functions
- Processes that are not covered by the current ITIL® 2011 Foundation syllabus are not discussed fully in this book but will be referenced where necessary for understanding.

How does the Service Lifecycle work?

ALTHOUGH THERE ARE FIVE STAGES throughout the Lifecycle, they are not separate, nor are the stages necessarily carried out in a particular order. The whole ethos of the Service Lifecycle approach is that each stage will affect the other, creating a continuous cycle. For this to work successfully, the Continuous Service Improvement (CSI) stage is incorporated throughout all of the other stages. Figure 3.C demonstrates some of the key outputs from each of the Service Lifecycle stages.

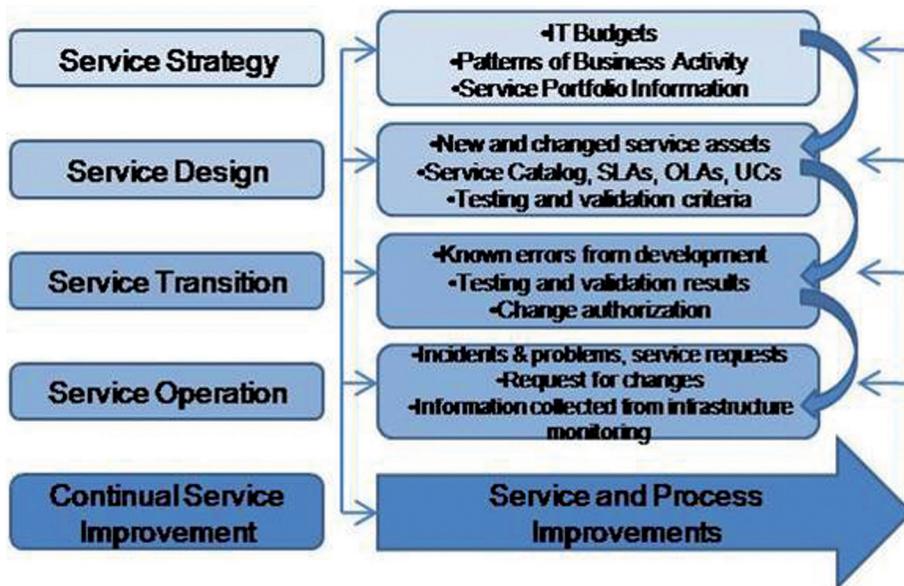


Figure 3.C—How Does the Service Lifecycle Work?

IT IS IMPORTANT TO NOTE that most of the processes defined do not get executed within only one lifecycle stage.

Service Strategy Stage: Determines the needs, priorities, demands, and relative importance for desired services and identifies the value being created through services and the predicted financial resources required to design, deliver, and support them.

Service Design Stage: Designs the infrastructure, processes, and support mechanisms needed to meet the availability requirements of the customer.

Service Transition Stage: Validates that the service meets the functional and technical fitness criteria to justify release to the customer.

Service Operation Stage: Monitors the ongoing availability being provided. During this stage, we also manage and resolve incidents that affect service availability.

Continual Service Improvement Stage: Coordinates the collection of data, information, and knowledge regarding the quality and performance of services supplied and Service Management activities performed. Service Improvement Plans developed and coordinated to improve any aspect involved in the management of IT services.

Chapter 4

SERVICE STRATEGY



Figure 4.A—Service Strategy

The Service Strategy stage is concerned predominantly with the development of capabilities for Service Management, enabling these practices (along with the IT organization in general) to become a strategic asset of the organization. The guidance provided by the volume can be summarized as:

- Understanding the principles of Service Strategy
- Developing Service Strategy within Service Management
- Developing strategies for services and services for strategies
- How strategy affects the Service Lifecycle
- Strategies for organizational and cultural change

Purpose of Service Strategy

THE PURPOSE OF THE SERVICE strategy stage of the service lifecycle is to define the perspective, position, plans, and patterns that a service provider needs to be able to execute to meet an organization's business outcomes.

The objectives of service strategy include providing:

- An understanding of what strategy is
- A clear identification of the definition of services and the customers who use them
- The ability to define how value is created and delivered
- A means to identify opportunities to provide services and how to exploit them
- A clear service provision model that articulates how services will be delivered and funded, to whom they will be delivered, and for what purpose
- The means to understand the organizational capability required to deliver the strategy
- Documentation and coordination of how service assets are used to deliver services and how to optimize their performance
- Processes that define the strategy of the organization, which services will achieve the strategy, what level of investment will be required, at what levels of demand, and the means to ensure a working relationship exists between the customer and service provider

By achieving these objectives, it will ensure that the IT organization has a clear understanding of how it can better support business growth, efficiency improvements, or other strategies that need to be realized.

KEY ROLE: To stop and think about WHY something has to be done before thinking about HOW.

Benefits of Service Strategy

SERVICE STRATEGY HAS THE POTENTIAL for many significant benefits to be delivered to the IT organization and the business/customers it serves. However, in many cases, these benefits fail to be realized due to insufficient connection and interfaces with other elements of the Service Lifecycle. For example:

The IT Strategy Group from an international banking and managed investment firm has decided to address the current economic downturn by reducing investments into the IT organization and Service Portfolio. As a result, the quality of some key services fall, with the support organization struggling to respond effectively to all calls for assistance. After a few months of lowered quality of service, the organization loses a number of major customers to their primary competitors. In response to the loss of these customers, further budget reductions are planned to counter the decrease in revenue earned.

By failing to realize their customers' value perception of services through service quality, the organization became caught in a negative cycle with potentially serious long term consequences. The missing link between the decisions being made by the strategy group and the potential impact they may have on elements of service quality (in particular the support of services in this example) or service value is often a challenge when developing Service Strategy.

When developed successfully as part of a holistic IT Service Management implementation, effective Service Strategy can:

- Support the ability to link activities performed by the service provider to outcomes that are critical to internal or external customers. As a result, the service provider will be seen to be contributing to the value (and not just the costs) of the organization.
- Enable the service provider to have a clear understanding of what types and levels of service will make its customers successful and then organize itself optimally to deliver and support those services. The service provider will achieve this through a process of defining strategies and services, ensuring a consistent, repeatable approach to defining how value will be built and delivered, which is accessible to all stakeholders.
- Enable the service provider to respond quickly and effectively to changes in the business environment, ensuring increased competitive advantage over time

- Support the creation and maintenance of a portfolio of quantified services that will enable the business to achieve positive return on its investment in services
- Facilitate functional and transparent communication between the customer and the service provider so that both have a consistent understanding of what is required and how it will be delivered
- Provide the means for the service provider to organize itself so that it can provide services in an efficient and effective manner

Major Concepts

Creating Service Value

PERHAPS, HISTORICALLY, BOTH PROVIDERS AND customers have used price as the focal point for communication and negotiation, but it is this path that ultimately leads to a negative experience for both parties. One of the key mantras that exist for any modern service provider (IT or otherwise) is that it is essential to clearly establish value before you can attach a price to the services offered. This ensures a few key things:

- It avoids an apples to oranges comparison, which usually occurs with a price focal point
- It enables the service provider to distinguish their capabilities and differentiation from their competitors
- It clearly communicates to the customer what they can expect to receive as part of the delivery service

Providers of IT services need to take special appreciation of the concept of value creation and communication due to the many misunderstandings about technology on behalf of customers (and poor communication by their IT providers). To address this issue, a central theme throughout the Service Strategy stage is value creation through services.

To explain the concept of value creation, the example of an Internet Service Provider (ISP) will be used throughout the next few sections.

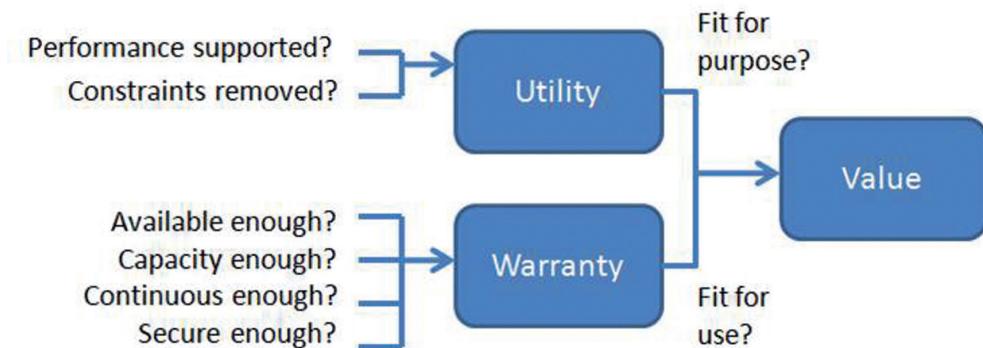


Figure 4.B—Creating Service Value

© Crown Copyright 2011 Reproduced under license from OGC

Important Formula: Service Warranty + Service Utility = Service Value

Service Utility describes the positive effect on business processes, activities, objects, and tasks. This could be the removal of constraints that improves performance or some other positive effect that improves the outcomes managed and focused on by the customer and business. This is generally summarized as being fit for purpose.

In the case of a service provided by an ISP, examples of Service Utility could be:

- Ability to shop and bank online
- Communicate easily with friends and family around the world without incurring an expensive phone bill
- Remove the need to always be at the office, instead allowing an individual to work or run their business from home

Service Warranty, on the other hand, describes how well these benefits are delivered to the customer. It describes the service's attributes, such as the availability, capacity, performance, security, and continuity levels to be delivered by the provider. Importantly, the Service Utility potential is only realized when the service is available with sufficient capacity and performance.

Examples of Service Warranty for the previously mentioned ISP are:

- The connection speed of the internet service
- The download quota provided (20GBs per month)
- The coverage of the service and network (e.g., for mobile broadband)
- The availability of support (e.g., 6am—10pm).

By describing both *Service Utility* and *Service Warranty*, it enables the provider to clearly establish the value of the service, differentiate themselves from the competition, and, where necessary, attach a meaningful price tag that has relevance to the customer and associated market space.

Service Packages and Service Level Packages

SOME CUSTOMERS HAVE HIGH UTILITY requirements, some have high warranty requirements, and some require high levels of both. To accommodate this, service providers can seek to satisfy one or more of these types of customers by packaging different levels of Service Utility and Service Warranty and pricing these packages accordingly.

To discuss Service Packages, Service Level Packages, and how they are used to offer choice and value to customers, we are going to use the example of the packages made available by typical Internet Service Providers (ISPs).

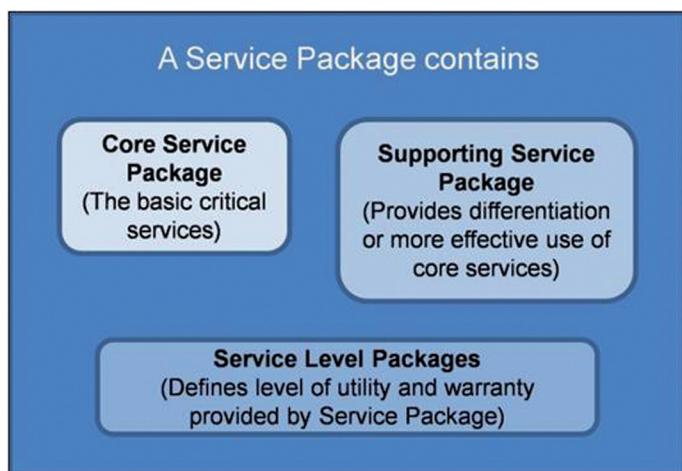


Figure 4.C—Service Package Example

A SERVICE PACKAGE PROVIDES A detailed description of a package of bundled services available to be delivered to customers. The contents of a Service Package includes:

- The core services provided
- Any supporting services provided
- The Service Level Package



Figure 4.D—Service Level Package Example

SERVICE LEVEL PACKAGES ARE EFFECTIVE in developing service packages with levels of utility and warranty appropriate to the customer's needs and in a cost-effective way.

- Availability and Capacity Levels
- Continuity Measures
- Security Levels
- Support arrangements (e.g., hours of support)

As customers, we have a wide range of choice when looking for an ISP to provide broadband internet. As a result, ISPs need to work hard to attract customers by communicating the value that they provide through their offerings. They also need to offer a wide range of choice for customers who have varying requirements and needs for their broadband internet service.

So for our ISP example, we can define a Service Package in the following way:

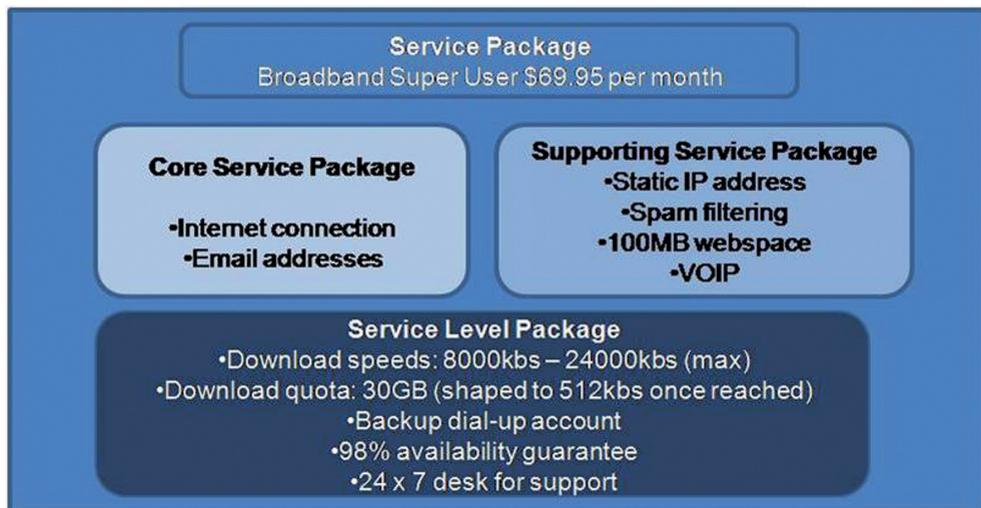


Figure 4.E—Detailed Service Package Example (ISP)

MOST OF THE COMPONENTS OF Service Packages and Service Level Packages are reusable components of the IT organization (many of which are services). Other components include software, hardware, and other infrastructure elements. By providing Service Level Packages in this way, it reduces the cost and complexity of providing services, while maintaining high levels of customer satisfaction. In our example above, the ISP can easily create multiple Service Packages with varying levels of Utility and Warranty provided in order to offer a wide range of choice to customers and to distinguish themselves from their competition.

The use of Service Packages and Service Level Packages enables Service Providers to avoid a one-size fits all approach to IT Services, while still maintaining efficiency of operations.

Service Assets

A **SERVICE ASSET** IS ANY resource or capability used in the provision of services. Organizations use them to create value in the form of goods and services for customers.

Resources	Capabilities
Input to a process is consumed and manipulated to produce an output	Used to coordinate, control, and deploy resources
Easy to acquire, can typically purchase or procure	Experience-driven, information-based, needs to develop and mature over time
Tangible, often a physical product	Intangible, often made up of behaviors and experience that has developed over time
Examples: IT Infrastructure, people, or money	Examples: Teams, processes, behaviors, knowledge

So WHILE IT IS RELATIVELY easy for an organization to increase the capacity of its infrastructure, it is far more difficult and complex to improve the organization's capabilities for managing capacity and performance in a cost-effective manner. Service Strategy should seek to optimize the use and implementation of Service Assets, according to the needs and objectives of the business.

Risk

RISK IS DEFINED AS UNCERTAINTY of outcome, whether it may result in a positive opportunity or negative threat. Managing risks requires the identification and control of the exposure to risk, which, if materialized, may have an impact on the achievement of an organization's business objectives. Every organization manages its risk but not always in a way that is visible, repeatable, and consistently applied to support decision-making.

This is true for many organizations, where one of the greatest risk factors is a lack of accurate information when making decisions. The goal of risk management is to ensure that the organization makes cost-effective use of a risk framework that has a series of well-defined steps. The aim is to support better decision-making through a good understanding of risks and their likely impact.

Service Strategy should seek to maintain the appropriate balance of risk and reward in regards to investments and capabilities invested and maintained for IT.

Service Strategy Processes

THE PROCESSES INCLUDED IN THE Service Strategy lifecycle stage are:

- Financial Management
- Service Portfolio Management
- Business Relationship Management
- Demand Management
- Strategy Management for IT Services

These processes work together to enable an IT organization to maximize the value of services being provided to customers and supply quality information to other ITSM processes. Although they are primarily strategic in nature, these processes also incorporate activities that are performed through all stages of the Service Lifecycle.

The ITIL® Foundation Certificate in ITSM syllabus and the corresponding exam requirements only cover three of these Service Strategy processes, the other processes are covered in the Intermediate level of study. Therefore, this book and the corresponding eLearning program will cover the following Service Strategy processes:

- Financial Management
- Service Portfolio Management
- Business Relationship Management

Financial Management

PURPOSE: THE PURPOSE OF FINANCIAL management for IT services is to secure the appropriate level of funding to design, develop, and deliver services that meet the strategy of the organization. At the same time, financial management for IT services is a gatekeeper that ensures the service provider does not commit to services that they are not able to provide. Financial management for IT services identifies the balance between the cost and quality of service and maintains the balance of supply and demand between the service provider and their customers.

For example, a customer asks an internal service provider to provide a service at a certain level. If the service provider is able to quantify the initial investment and ongoing costs of that service, the customer can make a decision as to whether that service will provide sufficient value to cover the costs. If the internal service provider

is not able to quantify the costs, then they will be put under significant pressure to deliver the service at the highest possible level.

Financial management enables the organization to manage its resources and to ensure that these resources are being used to achieve the organization's objectives.

Financial Management is focused on providing both the business and IT with improved insight (in financial terms) into the value of IT services, supporting assets, and operational management and support. This translates into improved operational visibility, insight, and superior decision-making at all levels of the organization.

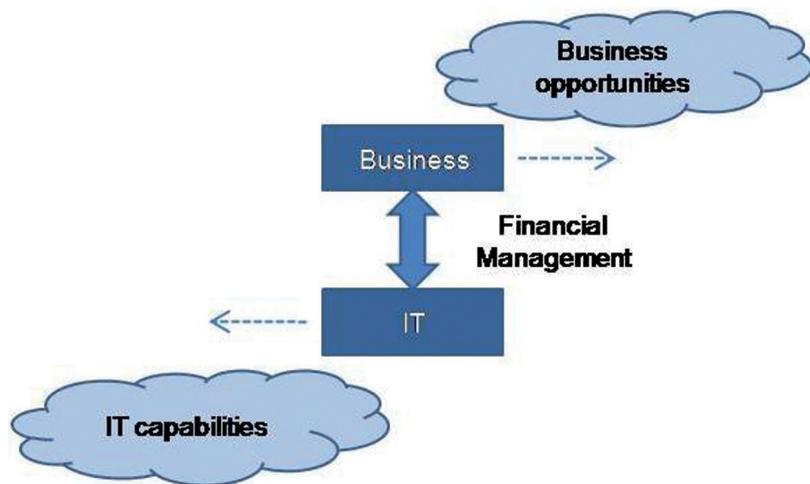


Figure 4.F—Financial Management Managing Conflicting Perspectives

WHEN IMPLEMENTED EFFECTIVELY, FINANCIAL MANAGEMENT provides the understanding and management of the distance and (sometimes) conflicting perspectives between the Business Desires/Opportunities and the Capabilities of the IT organization. It enables the business to be more IT conscious and IT to become more business - aligned.

As businesses evolve, markets change, and the IT industry matures, Financial Management is becoming increasingly adopted by IT organizations, with typical benefits including:

- Enhanced decision-making
- Increased speed of change
- Improved Service Portfolio Management
- Financial compliance and control
- Improved operational control
- Greater insight and communication of the value created by IT services

Terminology

Term	Definition
accounting	(<i>ITIL® Service Strategy</i>) The process responsible for identifying the actual costs of delivering IT services, comparing these with budgeted costs, and managing variance from the budget.
budget	A list of all the money an organization or business unit plans to receive and plans to pay out over a specified period of time. See also <i>budgeting</i> .
budgeting	The activity of predicting and controlling the spending of money. Budgeting consists of a periodic negotiation cycle to set future budgets (usually annual) and the day-to-day monitoring and adjusting of current budgets.
business case	(<i>ITIL® Service Strategy</i>) Justification for a significant item of expenditure. The business case includes information about costs, benefits, options, issues, risks, and possible problems.
charging	(<i>ITIL® Service Strategy</i>) Requiring payment for IT services. Charging for IT services is optional and many organizations choose to treat their IT service provider as a cost centre.
IT accounting	See <i>accounting</i> .

Scope

FINANCIAL MANAGEMENT IS NORMALLY A well-established and well-understood part of any organization. Professional accountants manage dedicated finance departments, which set financial policies, budgeting procedures, financial reporting standards, accounting practices, and revenue generation or cost recovery rules.

In an IT context, Financial Management is often a separate function either reporting to the CIO or the CFO but with some form of functional reporting between the two areas. Regardless of where the function is actually situated within the organization, Financial Management for IT services is a specialized area that requires an understanding of the world of finance and business as well as the world of technology.

A common misunderstanding is that all accountants are the same—without understanding that there are different specializations in accounting. Specifically, Financial Management for IT services requires accountants with a good understanding of cost accounting—a discipline often found in manufacturing environments. It is important that the correct skills are specified when hiring a person to manage IT finances.

Financial policies and practices within IT must be consistent with those of the rest of the organization. This is not only a requirement of most financial management legislation, regulations, and best practice, but it also facilitates better communication and reporting between IT and other business units.

In internal service providers, Financial Management plays a translational role between corporate financial systems and service management. The result of a service-oriented accounting function is that far greater detail and understanding is achieved regarding service provision and consumption and the generation of data that feeds directly into the planning process.

Activities

THERE ARE THREE FUNDAMENTAL ACTIVITIES for Financial Management for IT Services. These are:

- Budgeting
- IT Accounting
- Chargeback

Budgeting: Predicting the expected future requirements for funds to deliver the agreed upon services and monitoring adherence to the defined budgets. This ensures that the required resources to fund IT are made available and can improve the business case for IT projects and initiatives.

IT Accounting: Enables the IT organization to account fully for the way its money is spent. The definition of Cost Models can be used to identify costs by customer, by service, by activity, or other logical groupings. IT Accounting supports more accurate budgeting and ensures that any charging method utilized is simple, fair, and realistic.

Chargeback: Charging customers for their use of IT services. Charging can be implemented in a number of ways in order to encourage more efficient use of IT resources. Notional charging is one particular option in which the costs of providing services to customers are communicated but no actual payment is required.

Other Terminology

FINANCIAL MANAGEMENT ASSISTS IN THE role of **Service Valuation**, which is used to help the business and the IT service provider agree on the value of the IT service. It determines the balance demonstrating the total cost of providing an IT service against the total value offered to the business by the service. As previously described, value in services is created by the combination of Service Utility and Service Warranty.

Inputs

THE MAJOR INPUTS TO FINANCIAL Management for IT services include:

- Policies, standards, and practices defined by legislation, regulators, and enterprise financial managers
- Generally Accepted Accounting Practices (GAAP) and local variations
- All data sources where financial information is stored, including the supplier database, configuration management system, the service portfolio, customer agreement portfolio, application portfolio, and project portfolio
- The service portfolio provides the structure of services that will be provided, which, in turn, will be the basis for the accounting system—since all costs (and returns) will ultimately be expressed in terms of the services provided.

Outputs

THE MAJOR OUTPUTS OF FINANCIAL Management for IT services include.

- **Service valuation:** This is the ability to understand the costs of a service relative to its business value.
- **Service investment analysis:** Financial management for IT services provides the information and history to enable the service provider to determine the value of the investment in a service. This information is used by the business to demonstrate the value they have realized in using the service to achieve their desired outcomes.
- **Compliance:** Regardless of the location of a service provider, or whether they are internal or external, financial data is subject to regulation and legislation. Financial management for IT services helps implement and enforce policies that ensure the organization is able to store and archive financial data, secure and control it, and make sure that it is reported to the appropriate people. IT Financial Management data specifically allows the executives of the organization to track the levels of investment in IT and ensure that the money is being used to achieve the overall organizational strategy, mitigate risks, and achieve the appropriate returns in a legal and ethical manner.
- **Cost optimization:** Cost optimization should not always be equated with cost savings. The goal of cost optimization is to make sure that

investments are appropriate for the level of service that the customers demand and the level of returns that are being projected.

- **Business impact analysis (BIA):** Business impact analysis (BIA) involves understanding the effect on the business if a service were not available. This enables the business to prioritize investments in services and service continuity. Financial management for IT services contributes to BIA by providing financial data and information to quantify the potential effect on the business. It also helps to quantify and prioritize the actions that need to be taken to prevent the impact from becoming reality.
- **Planning confidence:** Planning confidence is not a tangible output or plan—rather it refers to the level of confidence that service stakeholders have in the service provider being able to accurately forecast costs and returns. A lack of planning confidence results in a lack of confidence in the service provider, and, in many cases, an unwillingness by the business to invest in IT unless absolutely necessary.

Service Portfolio Management

THE PURPOSE OF SERVICE PORTFOLIO Management is to ensure that the service provider has the right mix of services to balance the investment in IT with the ability to meet business outcomes. It tracks the investment in services throughout their lifecycle and works with other service management processes to ensure that the appropriate returns are being achieved. In addition, it ensures that services are clearly defined and linked to the achievement of business outcomes, thus ensuring that all design, transition, and operation activities are aligned to the value of the services.

A Service Portfolio describes a provider's services in terms of business value. It includes the complete set of services managed by a service provider, providing a means for comparing service value across multiple providers. The portfolio is used to articulate business needs and the service provider's response to those needs. It is possible for a service provider to have multiple Service Portfolios depending on the customer groups that they support. The information contained within the portfolio is used to manage the entire lifecycle of all services, for one or more customers.

Terminology

Term	Definition
retire	(<i>ITIL® Service Transition</i>) Permanent removal of an IT service or other configuration item from the live environment. Being retired is a stage in the lifecycle of many configuration items.
return on investment (ROI)	(<i>ITIL® Continual Service Improvement</i>) (<i>ITIL® Service Strategy</i>) A measurement of the expected benefit of an investment. In the simplest sense, it is the net profit of an investment divided by the net worth of the assets invested.
risk	A possible event that could cause harm or loss or affect the ability to achieve objectives. A risk is measured by the probability of a threat, the vulnerability of the asset to that threat, and the impact it would have if it occurred. Risk can also be defined as uncertainty of outcome and can be used in the context of measuring the probability of positive outcomes as well as negative outcomes.
service catalog	(<i>ITIL® Service Design</i>) (<i>ITIL® Service Strategy</i>) A database or structured document with information about all live IT services, including those available for deployment. The service catalog 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.
service pipeline	(<i>ITIL® Service Strategy</i>) A 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.
service portfolio	(<i>ITIL® Service Strategy</i>) The 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 catalog (live or available for deployment), and retired services.

Scope

THE SCOPE OF SERVICE PORTFOLIO Management is all services a service provider plans to deliver, those currently delivered, and those that have been withdrawn from service. The primary concern of Service Portfolio Management is whether the service provider is able to generate value from the services. Service Portfolio Management

will, therefore, track investments in services and compare them to the desired business outcomes.

Internal service providers will need to work with the business units in the organization to link each service to the business outcomes before they can compare investment with returns. External service providers tend to evaluate value more directly, as each service needs to be able to generate revenue directly or support revenue-generating services. The generation of revenue in an efficient manner will, in turn, facilitate profitability.

Service Portfolio Management evaluates the value of services throughout their lifecycles and must be able to compare what newer services have offered over the retired services they have replaced.

Categories

SERVICES ARE GROUPED INTO THREE distinct categories in the Service Portfolio:

- Service Pipeline (services that have been proposed or are in development)
- Service Catalog (live services or those available for deployment)
- Retired Services (decommissioned services)

The information making up the Service Portfolio(s) will come from many sources, so possible implementations may make use of existing databases and other data repositories, document management systems, financial systems, project management documentation, the Service Catalog, and other relevant input areas. Where necessary, the various sources of information may be collated and communicated by means of an internet/intranet-based interface so that duplication does not occur and that appropriate levels of detail and accessibility can be controlled.



Figure 4.G—A Service Portfolio

By DELIVERING THE OBJECTIVES ABOVE, the Service Portfolio either answers or helps to answer the following strategic questions:

- Why should a customer buy these services?
- Why should they buy these services from us?
- What are the pricing or chargeback models?
- What are our strengths and weaknesses, priorities, and risks?
- How are resources and capabilities to be allocated?

Understanding their options helps senior executives to make informed investment decisions in service initiatives, taking into account appropriate levels of risks and rewards. These initiatives may cross business functions and may span short, medium, and longer timeframes.

Investment Categories and Budget Allocations

SERVICE INVESTMENTS ARE SPLIT AMONG 3 strategic categories:

Transform the Business (TTB):

TTB investments are focused on initiatives that enter new market spaces with new capabilities being developed.

Grow the business (GTB):

GTB investments are intended to grow the organization's scope of services or gain more customers within an existing market space.

Run the business (RTB):

RTB investments are centered on maintaining service operations.

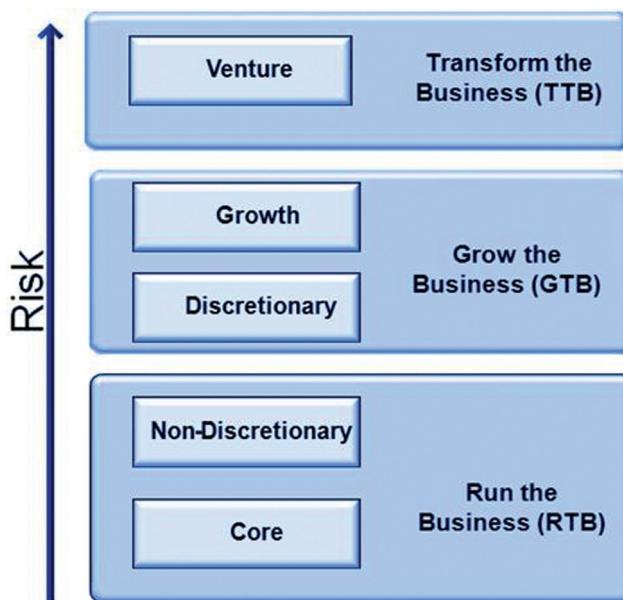


Figure 4.H—Balancing a Service Portfolio

© Crown Copyright 2011 Reproduced under license from OGC

Service Retirement

AN OFTEN OVER-LOOKED INVESTMENT, THIS is potentially one of the largest hidden costs in a service provider's organization, particularly in a large organization with a long history. Few providers have a clear plan for retiring increasingly redundant services. This is often due to a number of reasons, including a lack of visibility of what services are actually offered and the fear that retiring a service may impact other services being offered.

Refreshing the Portfolio

THE METHODS USED BY THE Service Portfolio Manager and other involved stakeholders seek to continually refresh the Service Portfolio, creating service investments that provide an optimum balance of risk and reward.

Changes occur to the conditions within every market space, invalidating previous Return on Investment (ROI) calculations. Some of these changes may be a result of:

- New competitors or alternative options entering a market
- The introduction of new compliance regulations
- Mergers and acquisitions
- New or changed public legislation
- Changes in the economic climate affecting various markets

The role of the Chief Information Officer (or other similar roles), in this context, is to monitor, measure, reassess and, rebalance investments as the markets and associated businesses change. They will need to identify what balance is appropriate for their organization (e.g., low risk and low reward, high risk and potential high reward) and authorize service investments that match these needs.

Activities

SERVICE PORTFOLIO MANAGEMENT CONSISTS OF four main phases of activity, illustrated in Figure 4.H

- **Define:** This phase focuses on documenting and understanding existing services and new services. Each service must have a documented business case. Data for each service, such as which service assets are required and where investments are made, needs to be validated.

- **Analyze:** The analysis of services in the portfolio will indicate whether the service is able to optimize value and how supply and demand can be prioritized and balanced.
- **Approve:** Every service needs to be approved and the level of investment authorized to ensure sufficient resources to deliver the anticipated levels of service.
- **Charter:** A charter is a document authorizing the project and stating its scope, terms, and references. Services are not just built on request from anyone in the organization. They have to be formally chartered and stakeholders need to be kept up-to-date with information about decisions, resource allocation, and actual investments made.

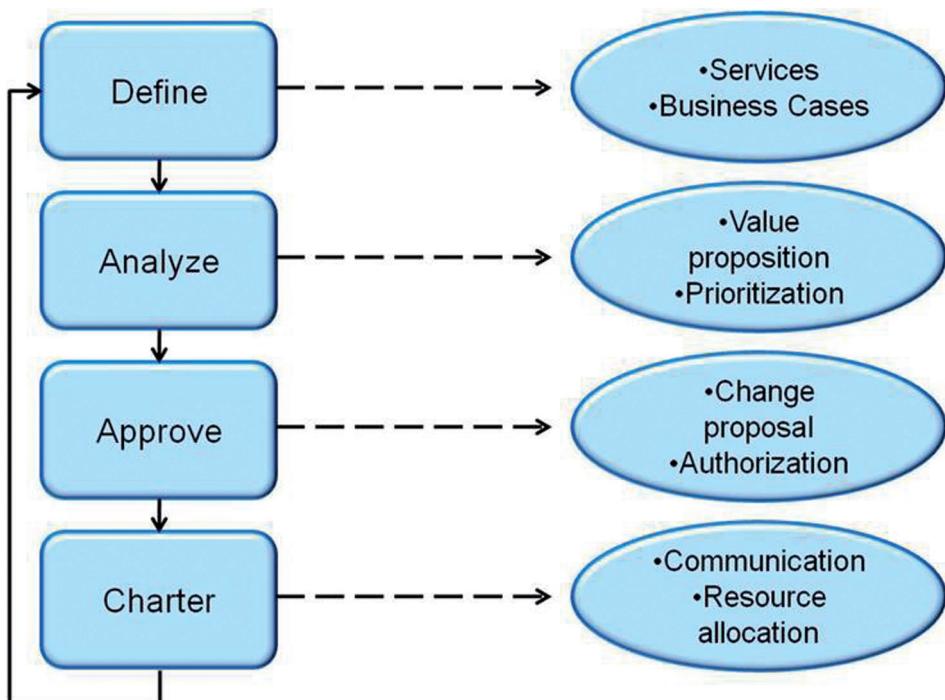


Figure 4.1—Phases of Service Portfolio Management Activities

© Crown Copyright 2011 Reproduced under license from OGC

Inputs

- Inputs to Service Portfolio Management include:
- Strategy plans
- Service improvement opportunities
- Financial reports
- Requests, suggestions, or complaints from the business
- Project updates for services in the charter stage of the process

Outputs

OUTPUTS FROM SERVICE PORTFOLIO MANAGEMENT include:

- An up-to-date service portfolio
- Service charters that authorize the work for designing and building new services or changes to existing services
- Reports on the status of new or changed services
- Reports on the investment made in services in the service portfolio and the returns on that investment
- Change proposals that are used to allow change management to assess and schedule the work and resources required to charter services
- Identified strategic risks

Business Relationship Management

FOR MANY ORGANIZATIONS, THE ROLE of the business relationship manager (BRM) was established to execute certain customer-facing activities in various processes, such as service level management. However, as the role matured it became clear that there was a discernable process to support that role.

Business Relationship Management is the process that enables BRMs to provide links between the service provider and customers at the strategic and tactical levels. The purpose of these links is to ensure that the service provider understands the business requirements of the customer and is able to provide services that meet these needs. The primary measure of whether this purpose is being achieved is the level of customer satisfaction.

The purpose of the Business Relationship Management process is two-fold:

- To establish and maintain a business relationship between the service provider and the customer based on understanding the customer and their business needs
- To identify customer needs and ensure that the service provider is able to meet these needs as business needs change over time and between circumstances. Business Relationship Management ensures that the service provider understands these changing needs. Business Relationship Management also assists the business in articulating the value of a service. Put another way, Business Relationship Management ensures that customer expectations do not exceed what they are willing to pay for and that the service provider is able to meet the customer's expectations before agreeing to deliver the service.

Terminology

Term	Definition
business relationship management	(ITIL® Service Strategy) The process responsible for maintaining a positive relationship with customers. Business relationship management identifies customer needs and ensures that the service provider is able to meet these needs with an appropriate catalog of services. This process has strong links with service level management.

Scope

FOR INTERNAL SERVICE PROVIDERS Business Relationship Management is typically executed between a senior representative from IT (larger organizations may have dedicated BRMs) and senior managers (customers) from the business units. Here, the emphasis is on aligning the objectives of the business with the activity of the service provider.

In external service providers, Business Relationship Management is often executed by a separate and dedicated function of BRMs or account managers—each one dedicated to a customer or group of smaller customers. The emphasis here is on maximizing contract value through customer satisfaction.

Business Relationship Management focuses on understanding how services meet customer requirements. To achieve this, the process must focus on understanding and communicating:

- Business outcomes that the customer wants to achieve
- Services that are currently offered to the customer and the way in which they are used by the customer
- The way in which services are currently offered, including who is responsible for the services, what levels of service have been agreed, the quality of services delivered, and any changes that are anticipated
- Technology trends that could impact current services and the customer, and the nature of the potential impact
- Levels of customer satisfaction and what action plans have been put in place to deal with the causes of dissatisfaction
- How to optimize services for the future
- How the service provider is represented to the customer. This at times means raising concerns around commitments that the business made to IT but is not meeting

Business Relationship Management depends on a number of other service management processes and functions. For example, the mapping of business outcomes and services is done in Service Portfolio Management. Service Level Management provides information about the levels of services agreed and achieved. Configuration Management provides a mapping of infrastructure, applications, services, service owners, and customers. Capacity Management provides information about utilization levels and the potential impacts of new technologies.

Unless the relationships between Business Relationship Management and other service management processes are clearly identified, there is potential for confusion about the boundaries between them. The main criterion for setting these boundaries is that Business Relationship Management focuses on the actual relationship between the service provider and its customers and the levels of customer satisfaction, whereas the other processes focus on the services themselves and the extent to which they meet the stated requirements.

The value of Business Relationship Management is in the ability of the service provider to articulate and meet the business needs of its customers. Business Relationship Management creates a forum for ongoing, structured communication with its customers. This enables Business Relationship Management to achieve better

alignment and integration of services in the future, as well as the ability to achieve the current business outcomes.

With that communication comes a greater understanding by the service provider of its customer's business and greater understanding by the customer of the service provider's capabilities and services. It helps to set realistic customer expectations and puts a human face to the service provider.

When there are disagreements about what should be delivered, Business Relationship Management enables both groups to reach agreement quickly and without speculation about motives that often occur when two parties do not know each other. The end result is higher levels of trust that the service provider is going to deliver value in the future and a greater willingness to work together as strategic partners.

The focus on customer satisfaction enables the service provider and customer alike to gauge how effectively the business objectives are being met.

Without Business Relationship Management, services will still be delivered and will still meet delivery target, but it is difficult to quantify the value of the services and there is no guarantee that the appropriate business needs are being fully met, that services are prioritized correctly, or that the customers the service provider meets with are truly representing the business needs of the customer. Service provision without Business Relationship Management is possible, but it is costly, erratic, and filled with mistrust.

Activities

THE TWO OVERARCHING ACTIVITIES OF the Business Relationship Management process are:

- To represent the service provider to its customers through coordinated marketing, selling, and delivery activities
- To work with Service Portfolio Management and design coordination to ensure that the service provider's response to customer requirements is appropriate. Thus, the process facilitates customer advocacy throughout the Service Lifecycle.

Inputs

INPUTS TO BUSINESS RELATIONSHIP MANAGEMENT include:

- Customer requirements
- Customer requests, complaints, escalations, or compliments
- The service strategy
- Where possible, the customer's strategy
- The service portfolio
- The project portfolio to ensure that requirements are gathered in a timely fashion and that all projects include Business Relationship Management activity where appropriate
- Service Level Agreements
- Requests for change
- Patterns of business activity and user profiles defined by Demand Management and that need to be validated through Business Relationship Management

Outputs

OUTPUTS OF BUSINESS RELATIONSHIP MANAGEMENT include:

- Stakeholder definitions
- Defined business outcomes
- Agreement to fund (internal) or pay for (external) services
- The customer portfolio
- Service requirements for strategy, design, and transition
- Customer satisfaction surveys and the published results of these surveys
- Schedules of customer activity in various service management process activities
- Schedule of training and awareness events
- Reports on the customer perception of service performance

Service Strategy Summary

THE SERVICE STRATEGY STAGE ENABLES the organization to ensure that the organizational objectives for IT are defined and that Services and Service Portfolios are maximized for value.

Other benefits delivered include:

- Enhanced ability to predict the resources required to fund IT
- Clearer visibility of the costs for providing IT Services
- Quality information to support investment decisions in IT
- Understanding of the use and demand for IT Services with the ability to influence positive and cost-effective use of IT

As the focal point for strategy, policy, and guidelines that direct the efforts and practices of the IT organization, Service Strategy has many important interfaces with the rest of the Service Lifecycle. Some of these include:

- **Interfaces with the Service Design stage:**
 - Service Archetypes and Models, which describe how service assets interact with customer assets. These are important high-level inputs that guide the design of services
 - Definition of business outcomes to be supported by services
 - Understanding of varying priority in required service attributes
 - Relative design constraints for the service (e.g., budget, contractual terms and conditions, copyrights, utility, warranty, resources, standards, and regulations etc.)
 - Definition of the cost models associated with providing services
- **Interfaces with the Service Transition stage:**
 - Service Transition provides evaluations of the costs and risks involved with introducing and modifying services. It also provides assistance in determining the relative options or paths for changing strategic positions or entering market spaces.
 - Request for Changes may be utilized to affect changes to strategic positions
 - Planning of the required resources and evaluation of whether the change can be implemented fast enough to support the strategy
 - Control and recording of service assets is maintained by Service Asset and Configuration Management

- **Interfaces with the Service Operation stage:**
 - Service Operation will deploy service assets in patterns that most effectively deliver the required utility and warranty in each segment across the Service Catalog
 - Deployment of shared assets that provide multiple levels of redundancy, support a defined level of warranty, and build economies of scale
 - Service Strategy must clearly define the warranty factors that must be supported by Service Operation with attributes of reliability, maintainability, redundancy, and overall experience of availability
- **Interfaces with the Continual Service Improvement stage:**
 - Continual Service Improvement (CSI) will provide the coordination and analysis of the quality, performance, and customer satisfaction of the IT organization, including the processes utilized and services provided
 - Integration with CSI will also provide the identification of potential improvement actions that can be made to elements of Service Strategy

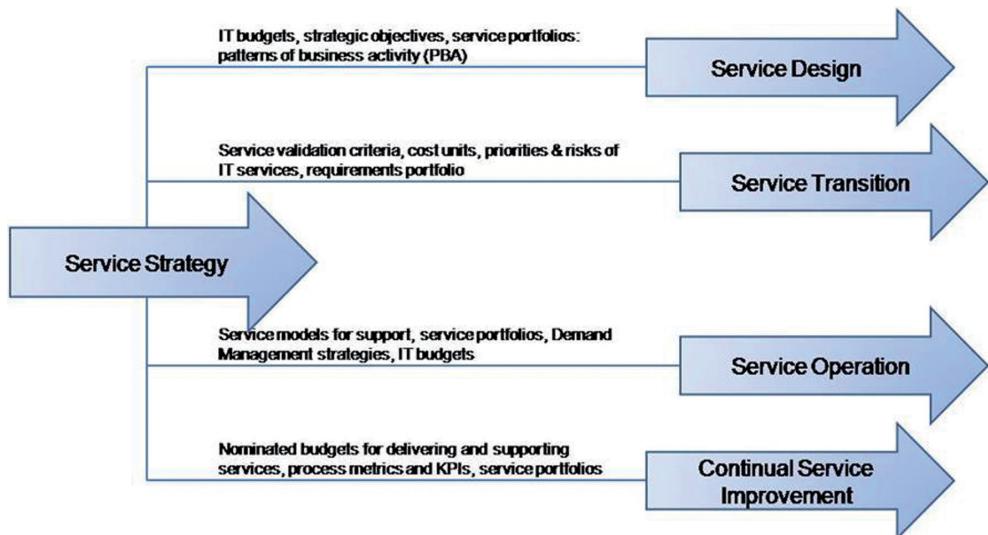


Figure 4.J—Some Service Strategy Outputs to Other Lifecycle Stages

Service Strategy Scenario

To ASSIST WITH YOUR LEARNING and understanding of how the stages and processes work together, the following scenario will be used throughout this book.

This simplistic overview of a service gives examples of how the processes are utilized to create the service.

The business has requested that they would like to be able to use the internet for instant messaging with international offices. They are also interested in VOIP and video conferencing. We will call this new service HYPE. This scenario will continue throughout the rest of the book.

Overall Service Strategy

- It is important here to truly understand exactly what the business needs are, as well as their expectations for this service
- Value must be defined (remember that utility + warranty = value):
 - Utility considers the features of HYPE—what type of support will the business require?, what features will the business want/need?, i.e., is it fit for purpose?
 - Warranty considers the levels of service guarantee (e.g., continuity, availability, security, capacity) that the business requires to be clarified—this is set out in service level packages
- Service Level Packages:
 - Core service package—instant messaging
 - Supporting service package—added VOIP and/or video conferencing, ability to attach files
 - Service Level packages—video quality, security of transmissions, access times, service support, user access

Financial Management Considerations

- Cost to purchase/build service
- Cost of hardware (web cams, PC upgrades if necessary)
- Cost of increased internet access/bandwidth
- Charging for service?
- Budget?

Service Portfolio Management Considerations

- You have already been trialing X brand instant messenger service among the IT staff, so an entry has been added to the Service Pipeline
- Are there redundant services to retire?

Business Relationship Management Considerations

- Service portfolio and customer portfolio
- Customer satisfaction surveys and measures
- Documented business outcomes and customer requirements

By determining the above before you start to design the service, you are in a better position to ensure that HYPE will meet the customer needs (closed loop system). Remember, this is where value is agreed and Service Operation is where the value of HYPE is seen. As we all know, the level of value will more than likely be in direct correlation to the dollars the business is prepared to pay and this is why it is important to clarify this now, before we start designing.

Service Strategy Review Questions

THESE QUESTIONS ALSO COVER THE Introduction and Common Terminology Chapters.

Question 1

Which ITIL® process is responsible for developing a charging system?

- a) Availability Management
- b) Capacity Management
- c) Financial Management for IT Services
- d) Service Level Management

Question 2

What is the RACI model used for?

- a) Documenting the roles and relationships of stakeholders in a process or activity
- b) Defining requirements for a new service or process
- c) Analyzing the business impact of an incident
- d) Creating a balanced scorecard showing the overall status of Service Management

Question 3

Which of the following identifies two Service Portfolio components within the Service Lifecycle?

- a) Catalog Service Knowledge Management System and Requirements Portfolio
- b) Service Catalog and Service Pipeline
- c) Service Knowledge Management System and Service Catalog
- d) Service Pipeline and Configuration Management System

Question 4

Which of the following is NOT one of the ITIL® core publications?

- a) Service Operation
- b) Service Transition
- c) Service Derivation
- d) Service Strategy

Question 5

A Service Level Package is best described as?

- a) A description of customer requirements used to negotiate a Service Level Agreement
- b) A defined level of utility and warranty associated with a core service package
- c) A description of the value that the customer wants and for which they are willing to pay
- d) A document showing the service levels achieved during an agreed reporting period

Question 6

Setting policies and objectives is the primary concern of which of the following elements of the Service Lifecycle?

- a) Service Strategy
- b) Service Strategy and Continual Service Improvement
- c) Service Strategy, Service Transition, and Service Operation
- d) Service Strategy, Service Design, Service Transition, Service Operation, and Continual Service Improvement

Question 7

A service owner is responsible for which of the following?

- a) Designing and documenting a service
- b) Carrying out the service operations activities needed to support a service
- c) Producing a balanced scorecard showing the overall status of all services
- d) Recommending improvements

Question 8

The utility of a service is best described as:

- a) Fit for design
- b) Fit for purpose
- c) Fit for function
- d) Fit for use

Question 9

The warranty of a service is best described as:

- a) Fit for design
- b) Fit for use
- c) Fit for purpose
- d) Fit for function

Question 10

The contents of a service package includes:

- a) Base Service Package, Supporting Service Package, Service Level Package
- b) Core Service Package, Supporting Process Package, Service Level Package
- c) Core Service Package, Base Service Package, Service Support Package
- d) Core Service Package, Supporting Services Package, Service Level Package

Chapter 5

SERVICE DESIGN



Figure 5.A—Service Design

The Service Design stage is concerned predominantly with the design of IT Services, as well as the associated or required:

- Processes
- Service management information systems and tools
- Service solutions
- Technology architectures
- Measurement systems

The driving factor in the design of new or changed services is the support of changing business needs. Every time a new service solution is produced, it needs to be checked against the rest of the Service Portfolio to ensure that it will integrate and interface with all of the other services in existence.

Purpose and Value

THE PURPOSE OF THE SERVICE Design stage of the lifecycle is to design IT services, together with the governing IT practices, processes, and policies to realize the service provider's strategy and to facilitate the introduction of these services into supported environments, ensuring quality service delivery, customer satisfaction, and cost-effective service provision.

In ITIL® 2011, it is understood that the focus on business processes supported and business value provided is a fundamental principle of IT Service Management. With this focus, the impact of technology on the business and how business change may impact technology can both be predicted. The creation of a totally integrated Service Catalog—including business units, processes, and services and their relationships and dependencies on IT services, technology, and components—is crucial to increasing the IT service provider's capability to meet the business's needs. All aspects of Service Design are vital elements in supporting and enhancing the capability of the IT service provider, particularly the design of the service portfolio, the service catalog, and

the individual IT services. All of these activities will also improve the alignment of IT service provision with the business's goals and its evolving needs.

The business focus in ITIL® IT service management (ITSM) enables an IT service provider organization to:

- Align IT service provision with business goals and objectives
- Prioritize all IT activities based on business impact and urgency, ensuring critical business processes and services receive the most attention
- Increase business productivity and profitability through the increased efficiency and effectiveness of IT processes
- Support the requirements for corporate governance with appropriate IT governance and controls
- Create competitive advantage through the exploitation and innovation of IT infrastructure as a whole
- Improve service quality, customer satisfaction, and user perception
- Ensure regulatory and legislative compliance
- Ensure appropriate levels of protection on all IT and information assets
- Ensure that IT services continue to be aligned with changing business needs over time

The Four Perspectives (Attributes) of ITSM

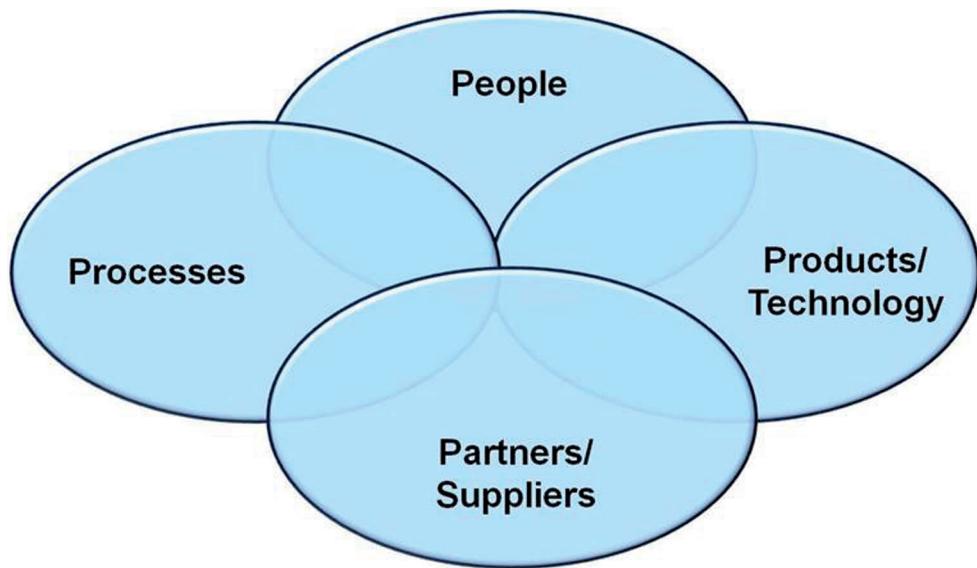


Figure 5.B—Four Perspectives (Attributes) of ITSM

THERE ARE FOUR PERSPECTIVES (**4P's**) or attributes that are important to consider in order for IT Service Management to be successful.

Partners/Suppliers Perspective: Takes into account the importance of Partner and External Supplier relationships and how they contribute to Service Delivery. It will help to ensure that suppliers deliver value for money and provide services that are clearly aligned to business requirements.

People Perspective: Concerned with the soft side of ITSM. This requires IT staff, customers, and other stakeholders to understand the purpose of ITSM and how it should be used within the organization. Training and education should be provided to ensure staff members have the correct skills, knowledge, and motivation to perform their roles.

Products/Technology Perspective: Takes into account the quality of IT services themselves and all technology architectures (hardware and software) required to provision them. Technology should be leveraged to both support and drive strategic opportunities for the business.

Process Perspective: Relates to the end-to-end delivery of services based on process flows. By having clearly established processes (with documentation, guidelines, and other supporting tools), it will enable a more consistent, repeatable, and measurable approach to the management of services.

Quality IT Service Management ensures that all of these four perspectives are taken into account as part of the continual improvement of the IT organization. It is the same when designing new or modified services in that these four perspectives need to be considered and catered for in order to enable success in its design, transition, and eventual use by customers.

Major Concepts

AN OVERALL, INTEGRATED APPROACH SHOULD be adopted for the design activities, covering five major aspects of Service Design:

- **Service solutions for new or changed services:** The requirements for new or changed services are extracted from the service portfolio. Each requirement is analyzed, documented, and agreed and a solution design is produced that is then compared with the strategies and constraints from Service Strategy to ensure that it conforms to corporate and IT policies. The design must ensure that this new or changed service is consistent with all other services and that all other services that interface with, underpin, or depend on the new or changed service are consistent with the new service. If not, either the design of the new service or the other existing services will need to be adapted. Each individual service solution design is also considered in conjunction with each of the other four aspects of service design.
- **The management information systems and tools, especially the service portfolio:** The management information systems and tools should be reviewed to ensure they are capable of supporting the new or changed service.
- **The technology architectures and management architectures:** These are reviewed to ensure that all the technology architectures and management architectures are consistent with the new or changed service and have the capability to operate and maintain the new service. If not, then either the architectures will need to be amended or the design of the new service will need to be revised.

- **The processes required:** These are reviewed to ensure that the processes, roles, responsibilities, and skills have the capability to operate, support, and maintain the new or changed service. If not, the design of the new service will need to be revised or the existing process capabilities will need to be enhanced. This includes all IT and service management processes, not just the processes involved in the Service Design stage itself.
- **The measurement methods and metrics:** These are reviewed to ensure that the existing measurement methods can provide the required metrics on the new or changed service. If not, then the measurement methods will need to be enhanced or the service metrics will need to be revised.

Completion of all of the above activities during the Service Design stage will ensure minimal issues arise during the subsequent stages of the Service Lifecycle. Therefore, Service Design must consolidate the key design issues and activities of all IT and Service Management processes within its own design activities to ensure that all aspects are considered and included within all designs for new or changed services as part of everyday process operation.

Service Design Packages

THE INFORMATION CONTAINED WITHIN A Service Design Package (SDP) includes documentation of all aspects of the service and its requirements in order to provide guidance and structure through all of the subsequent stages of its lifecycle. The information contained within it should address the five major aspects of Service Design that were previously mentioned. A Service Design Package is typically produced for each new IT service, major change, or IT service retirement.

Service Design Packages

- Business Requirements
- Service Applicability
- Service Contacts
- Service Functional Requirements
- Service Level Requirements
- Service Design and Topology

- Organizational Readiness Assessment
- User Acceptance Test Criteria
- Service Program
- Service Transition Plan
- Service Operational Plan
- Service Acceptance Criteria

Service Design Processes

THE PROCESSES INCLUDED WITH THE Service Design lifecycle stage are:

- Design Coordination
- Service Level Management
- Capacity Management
- Availability Management
- IT Service Continuity Management
- Information Security Management
- Supplier Management
- Service Catalog Management

It is important to note that many of the activities from these processes will occur in other lifecycle stages, especially Service Operation. Additionally, Service Level Management also plays an important role in Continual Service Improvement.

Like all ITIL® processes, the level to which the Service Design processes are required to be implemented will depend on many factors, including:

- The complexity and culture of the organization
- The relative size, complexity, and maturity of the IT infrastructure
- The type of business and associated customers being served by IT
- The number of services, customers, and end users involved
- Regulations and compliance factors affecting the business or IT
- The use of outsourcing and external suppliers for small or large portions of the overall IT Service Delivery

Based on these influencing factors, the design team may comprise of a single person in a small IT department or a worldwide network of business and customer oriented groups in an international organization.

Design Coordination

ONLY THROUGH WELL-COORDINATED ACTION CAN a service provider hope to create comprehensive and appropriate designs that will support the achievement of the required business outcomes.

The purpose of the design coordination process is to ensure the goals and objectives of the Service Design stage are met by providing and maintaining a single point of coordination and control for all activities and processes within this stage of the Service Lifecycle.

Terminology

Term	Definition
design coordination	(ITIL® Service Design) The process responsible for coordinating all service design activities, processes, and resources. Design coordination ensures the consistent and effective design of new or changed IT services, service management information systems, architectures, technology, processes, information, and metrics.

Scope

SOME DESIGN EFFORTS WILL BE part of a project, whereas others will be managed through the change process alone without a formally defined project. Some design efforts will be extensive and complex, while others will be simple and swift. Not every design activity requires the same level of rigor to ensure success, so a significant number of design efforts will require little or no individual attention from the design coordination process. Most design coordination process activity focuses around those design efforts that are part of a project, as well as those that are associated with changes of defined types. Typically, the changes that require the most attention from design coordination are major changes, but any change that an organization believes could benefit from design coordination may be included.

Each organization should define the criteria that will be used to determine the level of rigor or attention to be applied in design coordination for each design. Some organizations take the perspective that all changes, regardless of how small in scope, have a design stage, as it is important that all changes have clear and correct plans for how to implement them. Other organizations take the perspective that only changes that fit certain criteria, such as those associated with a project or major change, have a

formal Service Design stage. In this perspective, changes that fail to meet the agreed criteria may be considered out of the scope of this process.

Whichever perspective is adopted by an organization, the end result should be more successful changes that deliver the required business outcomes with minimal disruption or other negative impacts on business operations. If an organization's approach produces that result, then the organization is performing design coordination correctly.

The design coordination process includes:

- Assisting and supporting each project or other change through all the service design activities and processes
- Maintaining policies, guidelines, standards, budgets, models, resources, and capabilities for Service Design activities and processes
- Coordinating, prioritizing, and scheduling of all Service Design resources to satisfy conflicting demands from all projects and changes
- Planning and forecasting the resources needed for the future demand for Service Design activities
- Reviewing, measuring, and improving the performance of all Service Design activities and processes
- Ensuring that all requirements are appropriately addressed in service designs, particularly utility and warranty requirements
- Ensuring the production of service designs and/or SDPs and their handover to service transition

The design coordination process does not include:

- Responsibility for any activities or processes outside of the design stage of the service lifecycle
- Responsibility for designing the detailed service solutions themselves or the production of the individual parts of the SDPs. These are the responsibility of the individual projects or service management processes.

Activities

DESIGN COORDINATION ACTIVITIES FALL INTO two categories:

- **Activities relating to the overall Service Design lifecycle stage:** These activities include the development, deployment, and continual improvement of appropriate Service Design practices, as well as the coordination of actual design activity across projects and changes. These activities may be performed by design coordination process manager(s).
- **Activities relating to each individual design:** These activities focus on ensuring that each individual design effort and SDP, whether part of a project or simply associated with a change, conforms with defined practices and that they produce a design that will support the required business outcomes. These activities may be performed by a project manager or other individual with direct responsibility for the project or change, with the assistance and guidance of the design coordination process manager(s).

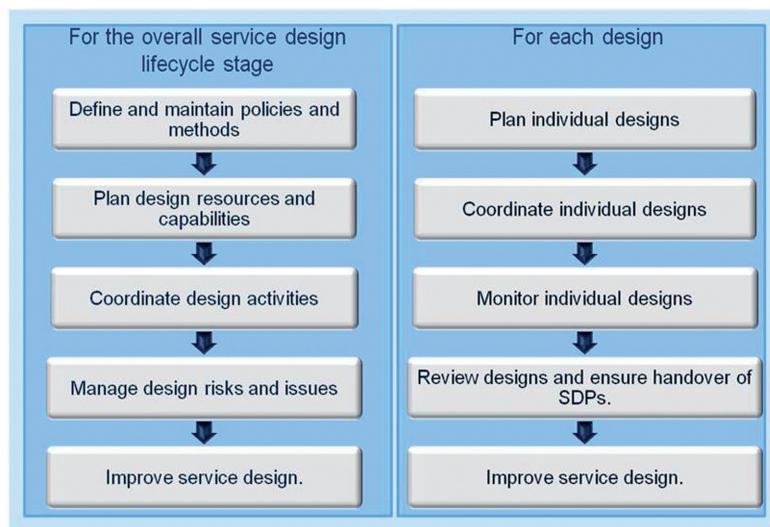


Figure 5.C—Design Coordination Activities

© Crown Copyright 2011 Reproduced under license from OGC

Inputs

A NUMBER OF SOURCES OF information are relevant to the design coordination process. These include:

- Service charters for new or significantly changed services
- Change requests from any stages of the Service Lifecycle
- Change records and authorized changes
- Business information from the organization's business and IT strategy, plans, and financial plans and information on their current and future requirements
- Business impact analysis, providing information on the impact, priority and risk associated with each service or changes to service requirements
- The service portfolio, including the service catalog and the business requirements for new or changed services in terms of service packages and service options
- The IT strategy and any associated constraints and resource limitations
- Governance requirements
- Corporate, legal, and regulatory policies and requirements
- The program and project schedule
- The schedule of change
- The configuration management system (CMS)
- Feedback from all other processes
- The enterprise architecture
- Management systems
- Measurement and metrics methods
- Processes

Outputs

THE PROCESS OUTPUTS OF DESIGN coordination are potentially:

- Comprehensive and consistent set of service designs and SDPs
- A revised enterprise architecture
- Revised management systems
- Revised measurement and metrics methods
- Revised processes
- Service portfolio updates
- Updates to change records

Service Level Management

Purpose

The purpose of the Service Level Management (SLM) process is to ensure that all current and planned IT services are delivered to agreed achievable targets. This is accomplished through a constant cycle of negotiating, agreeing, monitoring, reporting on, and reviewing IT service targets and achievements and through instigation of actions to correct or improve the level of service delivered.

While some organizations may continue to rely on a 'best endeavors' approach to service quality, the majority have realized that there needs to be a consistent, agreed, and understandable method used for defining and reporting of IT service quality. As the modern IT organization has matured over time to be more akin to any other area of business, there has also been an increased requirement for more formal methods by which the value of funding and investments into IT are assessed and performance measured for services provided and capabilities supported. Service Level Management is the process that seeks to provide consistency in defining the requirements for services, documenting targets and responsibilities, and providing clarity as to the achievements for service quality delivered to customers.

In effect, the process seeks to manage the grey areas that are formed between customers and the IT organization, as well as ensuring that the activities performed by various IT groups are coordinated optimally to meet customer requirements. The staff involved (Service Level Management team) are fluent in both technical and business jargon, they resolve disputes between parties (but as a result are sometimes seen as a spy in both camps), and generally work to improve the relationship between the IT organization and the customers it supports.

Terminology

Term	Definition
operational level agreement (OLA)	<p>(<i>ITIL® Continual Service Improvement</i>) (<i>ITIL® Service Design</i>) An agreement between an IT service provider and another part of the same organization. It supports the IT service provider's delivery of IT services to customers and defines the goods or services to be provided and the responsibilities of both parties. For example, there could be an operational level agreement:</p> <ul style="list-style-type: none"> • Between the IT service provider and a procurement department to obtain hardware in agreed times • Between the service desk and a support group to provide incident resolution in agreed times.
	See also service level agreement.
service improvement plan (SIP)	<p>(<i>ITIL® Continual Service Improvement</i>) A formal plan to implement improvements to a process or IT service.</p>
service level	<p>Measured and reported achievement against one or more service level targets. The term is sometimes used informally to mean service level target.</p>
service level agreement (SLA)	<p>(<i>ITIL® Continual Service Improvement</i>) (<i>ITIL® Service Design</i>) An agreement between an IT service provider and a customer. A service level agreement describes the IT service, documents service level targets, and specifies the responsibilities of the IT service provider and the customer. A single agreement may cover multiple IT services or multiple customers.</p>
	See also operational level agreement.
service level requirement (SLR)	<p>(<i>ITIL® Continual Service Improvement</i>) (<i>ITIL® Service Design</i>) A customer requirement for an aspect of an IT service. Service level requirements are based on business objectives and used to negotiate agreed service level targets.</p>
SLAM chart	<p>(<i>ITIL® Continual Service Improvement</i>) A service level agreement monitoring chart is used to help monitor and report achievements against service level targets. A SLAM chart is typically color-coded to show whether each agreed service level target has been met, missed, or nearly missed during each of the previous 12 months.</p>

underpinning contract (UC)	(<i>ITIL® Service Design</i>) A contract between an IT service provider and a third party. The third party provides goods or services that support delivery of an IT service to a customer. The underpinning contract defines targets and responsibilities that are required to meet agreed service level targets in one or more service level agreements.
----------------------------	--

Scope

SLM SHOULD PROVIDE A POINT of regular contact and communication to the customers and business managers of an organization in relation to service levels. In this context, it should represent the IT service provider to the business and the business to the IT service provider.

This activity should encompass both the use of existing services and the potential future requirements for new or changed services. SLM needs to manage the expectation and perception of the business, customers, and users and ensure that the quality (warranty) of service delivered by the service provider is matched to those expectations and needs. In order to do this effectively, SLM should establish and maintain SLAs for all current live services and manage the level of service provided to meet the targets and quality measurements contained within the SLAs. SLM should also produce and agree SLRs for all planned new or changed services that document warranty requirements.

This will enable SLM to ensure that all the services and components are designed and delivered to meet their targets in terms of business needs. The SLM process should include:

- Cooperation with the Business Relationship Management process; this includes development of relationships with the business as needed to achieve the SLM process objectives
- Negotiation and agreement of future Service Level Requirements and targets and the documentation and management of SLRs for all proposed new or changed services
- Negotiation and agreement of current Service Level Requirements and targets and the documentation and management of SLAs for all operational services
- Development and management of appropriate OLAs to ensure that targets are aligned with SLA targets

- Review of all supplier agreements and underpinning contracts with supplier management to ensure that targets are aligned with SLA targets
- Proactive prevention of service failures, reduction of service risks, and improvement in the quality of service, in conjunction with all other processes
- Reporting and management of all service level achievements and review of all SLA breaches
- Periodic review, renewal, and/or revision of SLAs, service scope, and OLAs as appropriate
- Identifying improvement opportunities for inclusion in the CSI register
- Reviewing and prioritizing improvements in the CSI register
- Instigating and coordinating SIPs for the management, planning, and implementation of service and process improvements

Agreements and Contracts

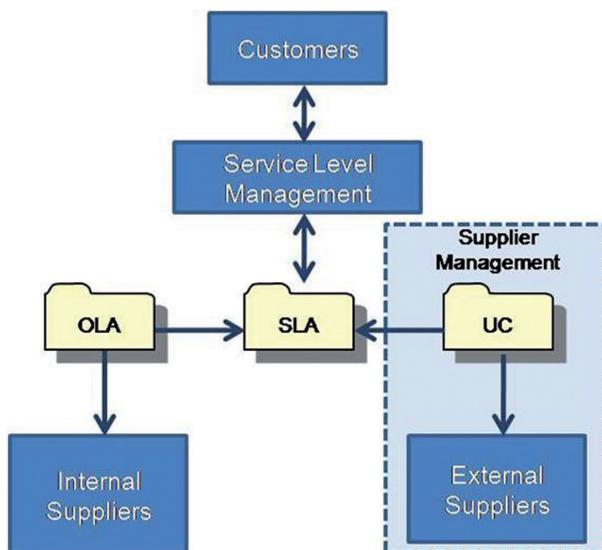


Figure 5.D—SLAs, OLAs, and UCs

NEGOTIATING AND AGREEING UPON THE SLAs and OLAs is the responsibility of Service Level Management. Supplier Management is responsible for negotiation and agreeing upon UCs with external suppliers. These two processes must communicate to ensure that the UCs do align with and support the SLAs in place.

What are the roles of OLAs and UCs?

They are agreements with other internal areas of the organization (e.g., the Service Desk, human resources) and external suppliers on how they support the IT organization in meeting the SLAs with customers.

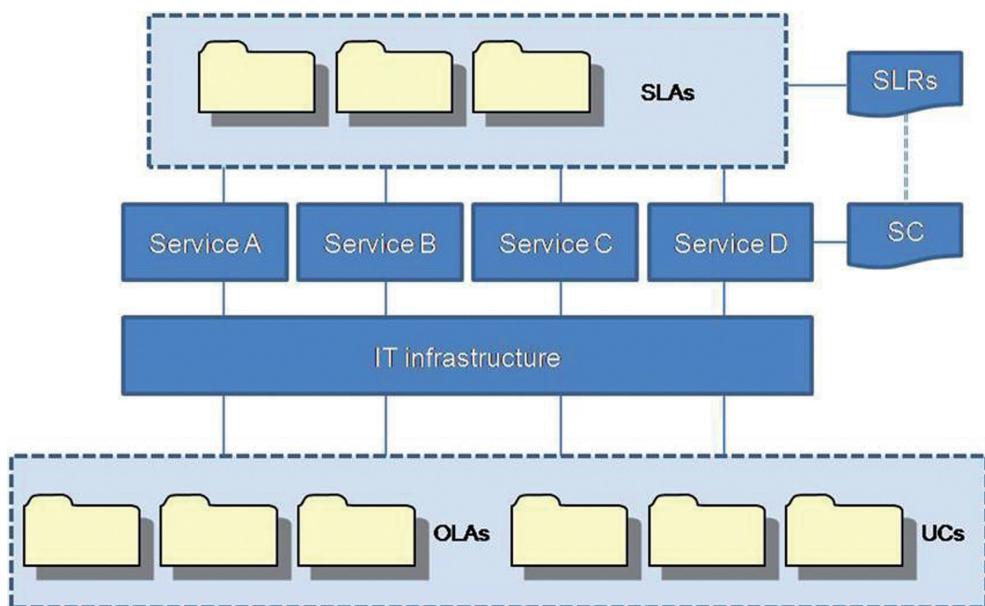


Figure 5.E—How SLAs, OLAs, and UCs Fit Together

Question:

An organization is planning to formalize its IT Service Management practices and wants to implement Service Level Management. At present, there is very little documentation of the services currently being provided to customers.

According to the ITIL® framework, which of these documents should be developed first?

Answer: Normally the Service Catalog should be produced first because we need to define and agree what we are providing and then we can map the customer requirements to the Service Catalog to see what gaps or redundant services exist. By rushing into the creation of SLAs, it is likely they will develop into complex or inaccurate representations of service levels and not help to manage the relationship between the service provider and customers.

Although Service Level Agreements are implemented in a wide variety of fashions, the guiding principle is that they are a written agreement between an IT service provider and the IT customer(s), defining the key service targets and responsibilities of both parties.

The key word here is agreement; SLAs should not be used as a way of holding one side or the other to ransom. When SLAs are viewed in a positive way—a way of continually improving the relationship between provider and customers—mutually beneficial agreements will be developed. Viewing SLAs as just contracts can contribute to development of a blame culture by both parties.

The level of technical detail included within the SLA will also vary, depending on the type and nature of the customer. Some customers may be an IT service provider themselves; others will be purely business-focused. To be successful in all of these scenarios, SLAs must be written in such a way that they are clear and unambiguous for both parties, leaving no room for confusion or misinterpretation. They certainly won't be perfect from the moment they are developed, so a continual cycle of review and revision should seek to improve the quality and effectiveness of SLAs over time.

Service Level Agreement Structures

THERE ARE A NUMBER OF ways in which SLAs can be structured. The important factors to consider when choosing the SLA structure are:

- Will the SLA structure allow flexibility in the levels of service to be delivered for various customers?
- Will the SLA structure require much duplication of effort?
- Who will sign the SLAs?

Three types of SLA structures that are discussed within ITIL® are service-based, customer-based, and multi-level or hierarchical SLAs.

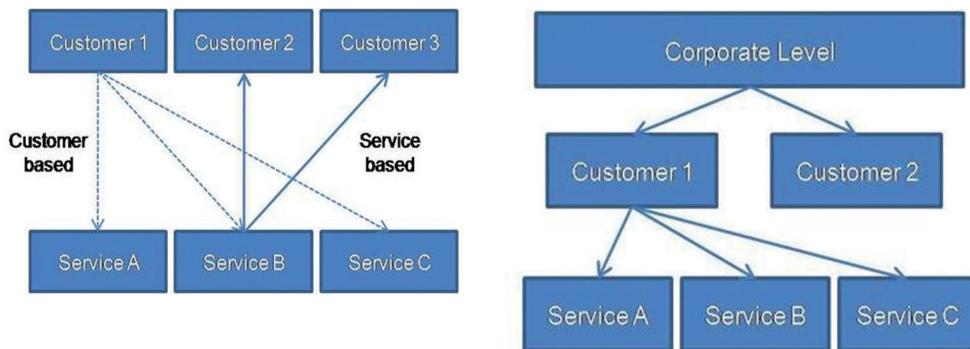


Figure 5.F—SLA Structures

MANY DIFFERENT FACTORS WILL NEED to be considered when deciding which SLA structure is most appropriate for an organization to use.

Typical Multi-Level SLA Structure Components:

1. **Corporate level:** All generic issues are covered, which are the same for the entire organization.

Example: The Corporate Security Baseline, e.g., Passwords, ID cards etc.

2. **Customer level:** Those issues specific to a customer can be dealt with.

Example: Security requirements of one or more departments within the organization are higher, e.g., the financial department needs higher security measures.

3. **Service level:** All issues relevant to a specific service (in relation to customer) can be covered.

Example: The email services for a particular department need encryption and secure backups.

Using a multi-level structure for a large organization reduces the duplication of effort, while still providing customization for customers and services (by inheritance).

The Typical Contents of SLAs

- An introduction to the SLA
- Service description
- Mutual responsibilities
- Scope of SLA
- Applicable service hours
- Service availability
- Reliability
- Customer support arrangements
- Contact points and escalation
- Service performance
- Batch turnaround times
- Security
- Costs and charging method used

The key criteria for any information to be contained within an SLA is that it must be measurable with all language used being clear and concise in order to aid understanding. As already discussed, SLAs should not only be used as legal documents for imposing penalties, otherwise it is in conflict with the goal of improving relationships between customers and the IT service provider. Another mistake made by organizations in implementing SLAs is that they become too long and technically-focused. When this occurs, there is potential for misunderstandings or for the SLA to go unread.

Service Level Management Activities

As an overview of Service Level Management, the process will generally consist of the following interrelated activities (*not necessarily in chronological order*):

1. Develop contacts and relationships
2. Design an SLA framework
3. Determine, document, and agree requirements for new services
4. Negotiate and develop SLAs
5. Review and revise SLAs, Underpinning Contracts, Operational Level Agreements, and service scope
6. Monitor service performance against SLAs
7. Produce service reports
8. Conduct service reviews and instigate improvements within an overall Service Improvement Plan (SIP)
9. Collate, measure, and improve customer satisfaction
10. Managing complaints and compliments

Service Improvement Plans

Service Improvement Plans are formal plans to implement improvements to a process or service. They are used to ensure that improvement actions are identified and carried out on a regular basis.

The identified improvements may come from:

- Breaches of Service Level Agreements
- Identification of user training and documentation issues
- Weak system testing
- Identified weak areas within internal and external support groups

Roles and Responsibilities

Service Level Manager:

- Must be senior enough to represent the organization with authority to do what is necessary
- Manages Service Catalog, SLAs, and OLAs and ensures alignment of Underpinning Contracts
- Identifies and manages improvements to services and processes

- Analyzes and reports on service level achievements

Skills: Relationship Management, patience, tolerance, resilience, and an understanding of the customer's business and how IT contributes to the delivery of that product or service.

Inputs

A NUMBER OF SOURCES OF information are relevant to the SLM process. These include:

- **Business information:** from the organization's business strategy, plans and financial plans, and information on its current and future requirements
- **BIA:** providing information on the impact, priority, risk, and number of users associated with each service
- **Business requirements:** details of any agreed, new, or changed business requirements
- **Strategies, policies, and constraints:** from Service Strategy
- **Service Portfolio and Service Catalog**
- **Change information, including RFCs:** from the Change Management process with a change schedule and a need to assess all changes for their impact on all services
- **CMS:** containing information on the relationships between the business services, the supporting services, and the technology
- **Customer and user feedback:** including complaints and compliments
- **Improvement opportunities:** from the CSI register
- **Other inputs:** including advice, information, and input from any of the other processes (e.g., Incident Management, Capacity Management and Availability Management), together with the existing SLAs, SLRs, and OLAs and past service reports on the quality of service delivered

Outputs

THE OUTPUTS OF SLM SHOULD include:

- **Service reports:** providing details of the service levels achieved in relation to the targets contained within SLAs. These reports should contain details of all aspects of the service and its delivery, including current and historical performance, breaches and weaknesses, major

events, changes planned, current and predicted workloads, customer feedback, and improvement plans and activities

- **Service improvement opportunities:** for inclusion in the CSI register and for later review and prioritization in conjunction with the CSI manager
- **SIP:** an overall program or plan of prioritized improvement actions, encompassing appropriate services and processes, together with associated impacts and risks
- **The service quality plan:** documenting and planning the overall improvement of service quality
- **Document templates:** standard document templates, format, and content for SLAs, SLRs, and OLAs, aligned with corporate standards
- **SLAs:** a set of targets and responsibilities should be documented and agreed within an SLA for each operational service
- **SLRs:** a set of targets and responsibilities should be documented and agreed within an SLR for each proposed new or changed service
- **OLAs:** a set of targets and responsibilities should be documented and agreed within an OLA for each internal support team
- **Reports:** on OLAs and underpinning contracts
- **Service review meeting minutes and actions:** all meetings should be scheduled on a regular basis with planned agendas and their discussions and actions recorded and progressed
- **SLA review and service scope review meeting minutes:** summarizing agreed actions and revisions to SLAs and service scope
- **Updated change information:** including updates to RFCs
- **Revised requirements for underpinning contracts:** changes to SLAs or new SLRs may require existing underpinning contracts to be changed or new contracts to be negotiated and agreed

Supplier Management

“No man is an island.”

THIS PHRASE COMES FROM A longer quotation by John Donne (1572-1631). The general meaning is that human beings do not thrive when isolated from others; we are all connected and, therefore, events and changes affecting one human being affect us all.

Although abstract, this concept provides an engaging way in which a service provider should approach the management of IT services. Like the original quote, *no service provider is an island*, so events and changes affecting their customers and suppliers will in turn have some consequence for them.

What does this mean for IT Service Management? Based on this principle, we need to ensure that we carefully evaluate, select, manage, and review any suppliers who will be involved in some way in the delivery and support of IT services and be sure to develop and foster the relationship in a mutually beneficial way. As many organizations have found out recently, the death of a supplier (caused by economic downturn) may mean their own future could be short lived.

Terminology

Term	Definition
supplier	<i>(ITIL® Service Design)</i> A third party responsible for supplying goods or services that are required to deliver IT services. Examples of suppliers include commodity hardware and software vendors, network and telecom providers, and outsourcing organizations. See <i>also</i> underpinning contract.
supplier and contract management information system (SCMIS)	<i>(ITIL® Service Design)</i> A set of tools, data, and information that is used to support supplier management. See <i>also</i> service knowledge management system.
underpinning contract (UC)	<i>(ITIL® Service Design)</i> A contract between an IT service provider and a third party. The third party provides goods or services that support delivery of an IT service to a customer. The underpinning contract defines targets and responsibilities that are required to meet agreed service level targets in one or more service level agreements.

Purpose

THE PURPOSE OF THE SUPPLIER Management process is to obtain value for money from suppliers and to provide seamless quality of IT service to the business by ensuring that all contracts and agreements with suppliers support the needs of the business and that all suppliers meet their contractual commitments.

The main objectives of the Supplier Management process are to:

- Obtain value for money from suppliers and contracts
- Ensure that contracts with suppliers are aligned to business needs and support and align with agreed targets in SLRs and SLAs, in conjunction with SLM
- Manage relationships with suppliers
- Manage supplier performance
- Negotiate and agree contracts with suppliers and manage them through their lifecycle
- Maintain a supplier policy and a supporting Supplier and Contract Management Information System (SCMIS)

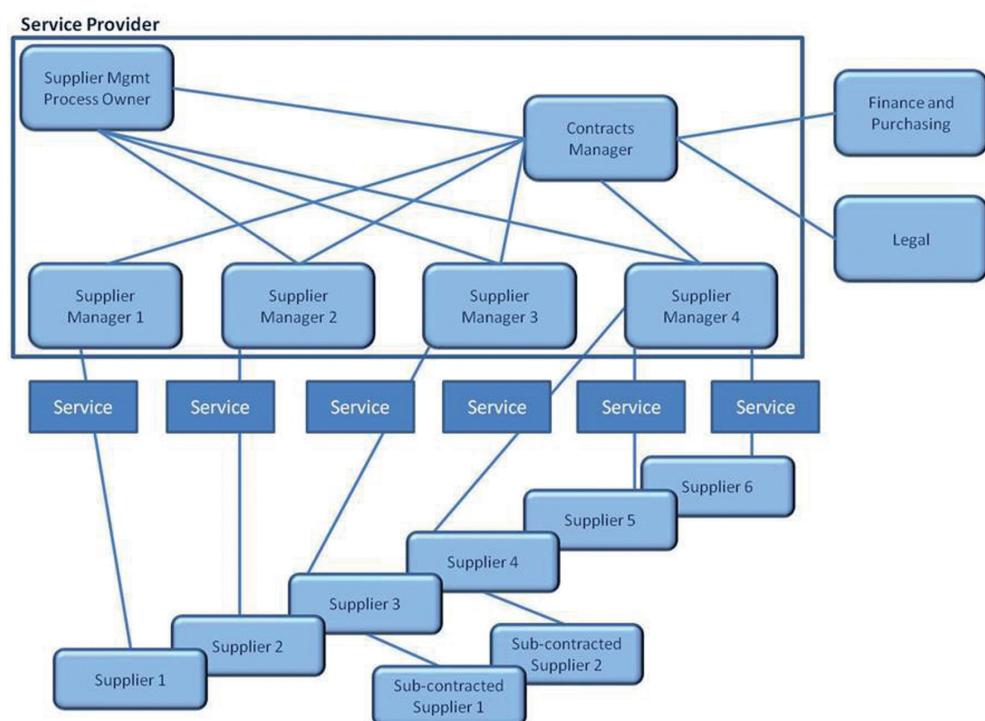


Figure 5.G—Roles and Interfaces for Supplier Management

© Crown Copyright 2011 Reproduced under license from OGC

Scope

THE SUPPLIER MANAGEMENT PROCESS SHOULD include the management of all suppliers and contracts needed to support the provision of IT services to the business. Each service provider should have formal processes for the management of all suppliers and contracts. However, the processes should adapt to cater for the importance of the supplier and/or the contract and the potential business impact on the provision of services. Many suppliers provide support services and products that independently have a relatively minor and fairly indirect role in value generation but collectively make a direct and important contribution to value generation and the implementation of the overall business strategy.

The greater the contribution the supplier makes to business value, the more effort the service provider should put into the management of the supplier and the more that supplier should be involved in the development and realization of the business strategy. The smaller the supplier's value contribution, the more likely it is that the relationship will be managed mainly at an operational level with limited interaction with the business. It may be appropriate in some organizations, particularly large ones, to manage internal teams and suppliers, where different business units may provide support of key elements.

The Supplier Management process should include:

- Implementation and enforcement of the supplier policy
- Maintenance of an SCMIS
- Supplier and contract categorization and risk assessment
- Supplier and contract evaluation and selection
- Development, negotiation, and agreement of contracts
- Contract review, renewal, and termination
- Management of suppliers and supplier performance
- Identification of improvement opportunities for inclusion in the CSI register and the implementation of service and supplier improvement plans
- Maintenance of standard contracts, terms, and conditions
- Management of contractual dispute resolution
- Management of sub-contracted suppliers

Activities

THE ACTIVITIES OF SUPPLIER MANAGEMENT can be summarized in this way:

- **Definition of new supplier and contract requirements:**
 - Identification of business need and preparation of the business case, including options (internal and external), costs, timescales, targets, benefits, risk assessment
 - Produce a statement of requirement (SoR) and/or invitation to tender (ITT)
 - Ensure conformance to strategy/policy
- **Evaluation of new suppliers and contracts:**
 - Identify method of purchase or procurement
 - Establish evaluation criteria—for example, services, capability (both personnel and organization), quality, and cost
 - Evaluate alternative options
 - Select
 - Negotiate contracts, targets, and the terms and conditions, including responsibilities, closure, renewal, extension, dispute, and transfer
 - Agree and award the contract
- **Supplier and contract categorization and maintenance of the SCMIS:**
 - Assessment or reassessment of the supplier and contract
 - Ensure changes progress through service transition
 - Categorization of the supplier
 - Update of SCMIS
 - Ongoing maintenance of the SCMIS
- **Establishment of new suppliers and contracts:**
 - Set up the supplier service and contract within the SCMIS and any other associated corporate systems
 - Transition of service
 - Establish contacts and relationships

- **Supplier, contract, and performance management:**
 - Management and control of the operation and delivery of service/products
 - Monitor and report (service, quality, and costs)
 - Review and improve (service, quality, and costs)
 - Management of the supplier and the relationship (communication, risks, changes, failures, improvements, contacts, interfaces)
 - Review, at least annually, service scope against business need, targets, and agreements
 - Plan for possible closure/renewal/extension
- **Contract renewal or termination**
 - Review (determine benefits delivered, ongoing requirement)
 - Renegotiate and renew or terminate and/or transfer
 - Transition to new supplier(s) or to internal resources

Supplier and Contact Management Information System (SCMIS):

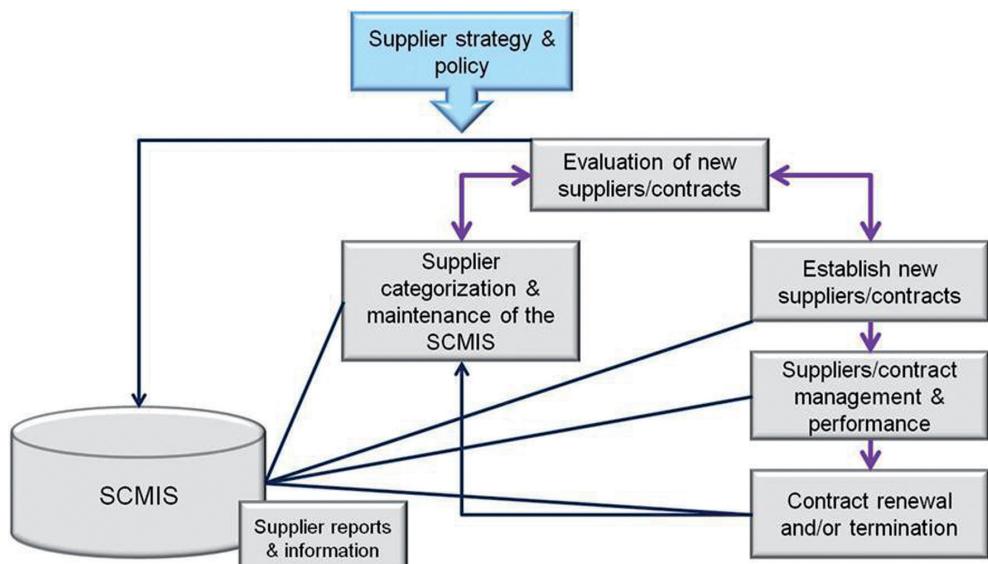


Figure 5.H—The Supplier and Contract Management Information System
 © Crown Copyright 2011 Reproduced under license from OGC

ALL SUPPLIER MANAGEMENT PROCESS ACTIVITY should be driven by supplier strategy and policy. In order to achieve consistency and effectiveness in the implementation of the policy, a Supplier and Contract Management Information System (SCMIS) should be established.

Ideally, the SCMIS should form an integrated element of a comprehensive CMS (Configuration Management System) or SKMS (Service Knowledge Management System), recording all supplier and contract details, together with the types of service, products etc. provided by each supplier and all the other information and relationships with other associated CIs (Configuration Items). This will also contribute to the information held in the Service Portfolio and Catalog.

Underpinning Contracts and Agreements

THE NATURE AND EXTENT OF an agreement between a service provider and supplier depends on the relationship type and an assessment of the risks involved. A pre-agreement risk assessment is a vital stage in establishing any external supplier agreement. For each party, it exposes the risks that need to be addressed and must be comprehensive and practical, covering a wide variety of risks, including financial, business reputation, operational, regulatory, and legal.

A comprehensive agreement minimizes the risk of disputes arising from a difference of expectations. A flexible agreement, which adequately caters for its adaptation across the term of the agreement, is maintainable and supports change with a minimum amount of renegotiation.

The contents of a basic Underpinning Contract or Service Level Agreement are:

- **Basic terms and conditions:** The term (duration) of the contract, the parties, locations, scope, definitions, and commercial basis
- **Service description and scope:** The functionality of the services being provided and its extent, along with constraints on the service delivery, such as performance, availability, capacity, technical interface, and security
- **Service standards:** The service measures and the minimum levels that constitute acceptable performance and quality—for example, IT may have a performance requirement to respond to a request for a new desktop system in 24 hours, with acceptable service deemed to have occurred where this performance requirement is met in 95% of cases. Service levels must be realistic, measurable, and aligned to the

organization's business priorities and underpin the agreed targets within SLRs and SLAs.

- **Workload ranges:** The volume ranges within which service standards apply or for which particular pricing regimes apply
- **Management information:** The data that must be reported by the supplier on operational performance—take care to ensure that management information is focused on the most important or headline reporting measures on which the relationship will be assessed
- **Responsibilities and dependencies:** Description of the obligations of the organization (in supporting the supplier in the service delivery efforts) and of the supplier (in its provision of the service), including communication, contacts, and escalation

Supplier Categorization

THE SUPPLIER MANAGEMENT PROCESS SHOULD be adaptive and spend more time and effort managing key suppliers than less important suppliers. This means that some form of categorization scheme should exist within the supplier management process to categorize the supplier and their importance to the service provider and the services provided to the business. Suppliers can be categorized in many ways, but one of the best methods for categorizing suppliers is based on assessing the risk and impact associated with using the supplier and the value and importance of the supplier and its services to the business, as illustrated in figure 5.H.

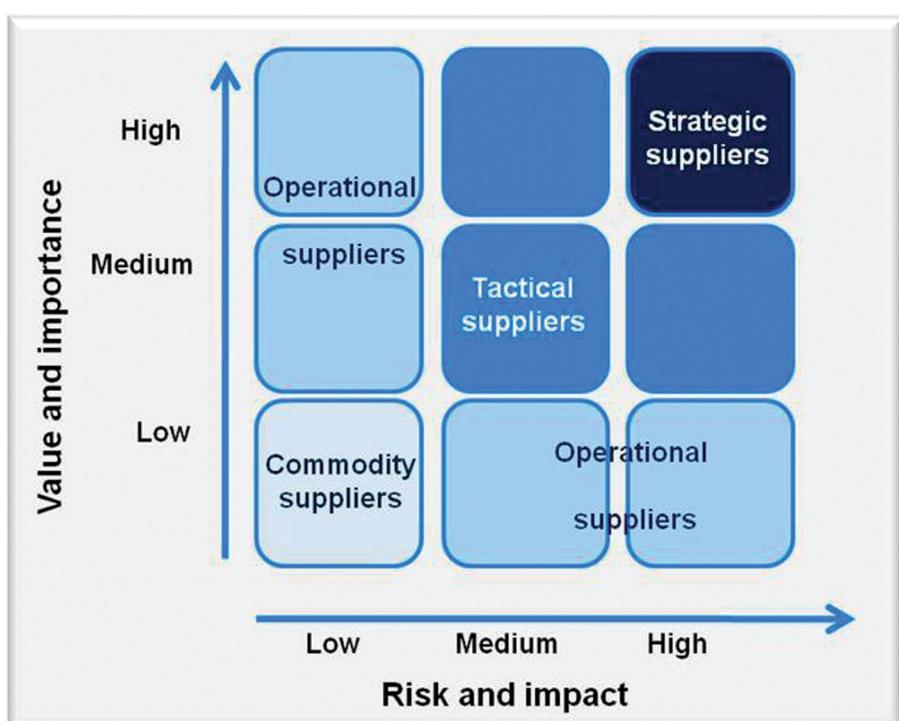


Figure 5.I—Supplier Categorization

© Crown Copyright 2011 Reproduced under license from OGC

THE AMOUNT OF TIME AND effort spent managing the supplier and the relationship can then be appropriate to its categorization:

- **Strategic:** for significant partnering relationships that involve senior managers sharing confidential strategic information to facilitate long-term plans. These relationships would normally be managed and owned at a senior management level within the service provider organization and would involve regular and frequent contact and performance reviews.
- **Tactical:** for relationships involving significant commercial activity and business interaction. These relationships would normally be managed by middle management and would involve regular contact and performance reviews, often including ongoing improvement programs (e.g., a hardware maintenance organization providing resolution of server hardware failures).
- **Operational:** for suppliers of operational products or services. These relationships would normally be managed by junior operational management and would involve infrequent but regular contact and performance reviews (e.g., an internet hosting service provider supplying hosting space for a low-usage, low-impact website or internally-used IT service).
- **Commodity:** for suppliers providing low-value and/or readily available products and services, which could be alternatively sourced relatively easily (e.g., paper or printer cartridge suppliers)

Strategically important supplier relationships are given the greatest focus. It is in these cases that supplier managers have to ensure the culture of the service provider organization is extended into the supplier domain so that the relationship works beyond the initial contract. The rise in popularity of outsourcing and the increase in the scope and complexity of some sourcing arrangements have resulted in a diversification of types of supplier relationships. At a strategic level, it is important to understand the options that are available so that the most suitable type of supplier relationship can be established to gain maximum business benefit and evolves in line with business needs.

Relationships with other Lifecycle Stages:

THE INFORMATION WITHIN THE SCD will provide a complete set of reference information for all Supplier Management procedures and activities needed across the Service Lifecycle. Such activities include:

Lifecycle Stage	Activities
Service Design	Evaluating which components of service provision should/could be provided by an external supplier or partner
	Supplier categorization and maintenance of the SCD
	Evaluation and set-up of new suppliers and contracts
Service Transition	Assessing the transition to new suppliers
	Establishing new suppliers
Service Operation	Ongoing Supplier and Contract Management and performance
	Contract renewal and termination
Continual Service Improvement	Identifying improvement actions involving suppliers
	Collating measurements gathered on supplier arrangements

This table shows that although Supplier Management is firmly placed within the Service Design Stage of the Lifecycle, many activities are carried out in the other Lifecycle Stages too.

Inputs

- **Business information:** from the organization's business strategy, plans and financial plans, and information on its current and future requirements
- **Supplier and contracts strategy:** this covers the sourcing policy of the service provider and the types of supplier and contract used. It is produced by the service strategy processes.
- **Supplier plans and strategies:** details of the business plans and strategies of suppliers, together with details of their technology developments, plans and statements, and information on their current financial status and projected business viability
- **Supplier contracts, agreements, and targets:** of both existing and new contracts and agreements from suppliers

- **Supplier and contract performance information:** of both existing and new contracts and suppliers
- **IT information: from the IT strategy and plans and current budgets**
- **Performance issues:** the Incident and Problem Management processes, with incidents and problems relating to poor contract or supplier performance
- **Financial information:** from Financial Management for IT services, the cost of supplier service(s) and service provision, the cost of contracts and the resultant business benefit, and the financial plans and budgets, together with the costs associated with service and supplier failure
- **Service information:** from the SLM process, with details of the services from the service portfolio and the service catalog, service level targets within SLAs and SLRs, and possibly from the monitoring of SLAs, service reviews, and breaches of the SLAs—also customer satisfaction data on service quality
- **CMS:** containing information on the relationships between the business, the services, the supporting services, and the technology

Outputs

THE OUTPUTS OF **SUPPLIER MANAGEMENT** are used within all other parts of the process by many other processes and by other parts of the organization. Often this information is supplied as electronic reports or displays on shared areas or as pages on intranet servers to ensure the most up-to-date information is always used. The information provided is as follows:

- **SCMIS:** This holds the information needed to execute the activities within Supplier Management—for example, the data monitored and collected as part of Supplier Management. This is then invariably used as an input to all other parts of the Supplier Management process.
- **Supplier and contract performance information and reports:** These are used as input to supplier and contract review meetings to manage the quality of service provided by suppliers and partners. This should include information on shared risk, where appropriate.
- **Supplier and contract review meeting minutes:** These are produced to record the minutes and actions of all review meetings with suppliers.
- **Supplier SIPs:** These are used to record all improvement actions and plans agreed between service providers and their suppliers, wherever

- they are needed, and should be used to manage the progress of agreed improvement actions, including risk reduction measures.
- **Supplier survey reports:** Often many people within a service provider organization have dealings with suppliers. Feedback from these individuals should be collated to ensure consistency in the quality of service provided by suppliers in all areas. These can be published as league tables to encourage competition between suppliers.

Service Catalog Management

IMAGINE WALKING INTO A RESTAURANT for lunch only to find there is no menu available for you to peruse. How will the staff provide you with information about what options are available to you? How will you know what ingredients and items are included with each meal? What will the price be of those meals? What about drinks or other items? Even if you manage to be served by a very efficient waiter who can recite everything to you flawlessly, how will you manage the large influx of information in such a small time and be able to choose what you want?

While this example may be far removed from the running of an IT organization the principles remain the same. A restaurant is in business to provide dining services to customers and through the use of their menu and the knowledge and skills of staff, customers can understand what is available to them and make effective choices in a simple manner. As an IT service provider, we are in the business of providing IT services to our customers, but what mechanisms do we use to make these transactions simple yet effective for all parties?

For most IT organizations, the Service Catalog provides this mechanism and, in many ways, it serves as the foundation for much of the work involved within the scope of Service Offerings and Agreements. Without some agreed definition of what services we offer, what those services provide, and which customers we provide them to, the development and management of Service Portfolios, Service Level Agreements, IT budgets, and other related items becomes all the more difficult and things only get worse as time progresses.

But it is not enough to simply have some form of Service Catalog. We must also seek to ensure that the Service Catalog is continually maintained and updated to contain correct, appropriate, and relevant information to assist communication and transactions with customers.

Terminology

Term	Definition
service catalog	<i>(ITIL® Service Design) (ITIL® Service Strategy)</i> A database or structured document with information about all live IT services, including those available for deployment. The service catalog 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.

Purpose

THE PURPOSE OF THE SERVICE Catalog Management process is to provide and maintain a single source of consistent information on all operational services and those being prepared to be run operationally and to ensure that it is widely available to those who are authorized to access it.

The objectives of the Service Catalogue Management process are to:

- Manage the information contained within the Service Catalog
- Ensure that the Service Catalog is accurate and reflects the current details, status, interfaces, and dependencies of all services that are being run, or being prepared to run, in the live environment, according to the defined policies
- Ensure that the Service Catalog is made available to those approved to access it in a manner that supports their effective and efficient use of Service Catalog information
- Ensure that the Service Catalog supports the evolving needs of all other service management processes for service catalog information, including all interface and dependency information.

Scope

THE SCOPE OF THE SERVICE Catalog Management process is to provide and maintain accurate information on all services that are being transitioned or have been transitioned to the live environment. The services presented in the Service Catalog may be listed individually or, more typically, some or all of the services may be

presented in the form of service packages (see *ITIL® Service Strategy* for information about service packages).

The Service Catalog Management process covers:

- Contribution to the definition of services and service packages
- Development and maintenance of service and service package descriptions appropriate for the Service Catalog
- Production and maintenance of an accurate Service Catalog
- Interfaces, dependencies, and consistency between the Service Catalog and the overall Service Portfolio
- Interfaces and dependencies between all services and supporting services within the Service Catalog and the CMS
- Interfaces and dependencies between all services, supporting components, and configuration items (CIs) within the Service Catalog and the CMS

The Service Catalog Management process does not include:

- Detailed attention to the capturing, maintenance, and use of service asset and configuration data as performed through the Service Asset and Configuration Management process (see *ITIL® Service Transition*)
- Detailed attention to the capturing, maintenance, and fulfillment of service requests as performed through request fulfillment (see *ITIL Service Operation*)

Depending on the number and complexity of services offered, the size of the customer and end user population, and what objectives have been defined for the process, these activities and items may have little or a great deal of reliance on technology to be effective.

Once the definition of services and their interfaces is finalized, the knowledge and information of the Service Catalog is logically divided into two aspects:

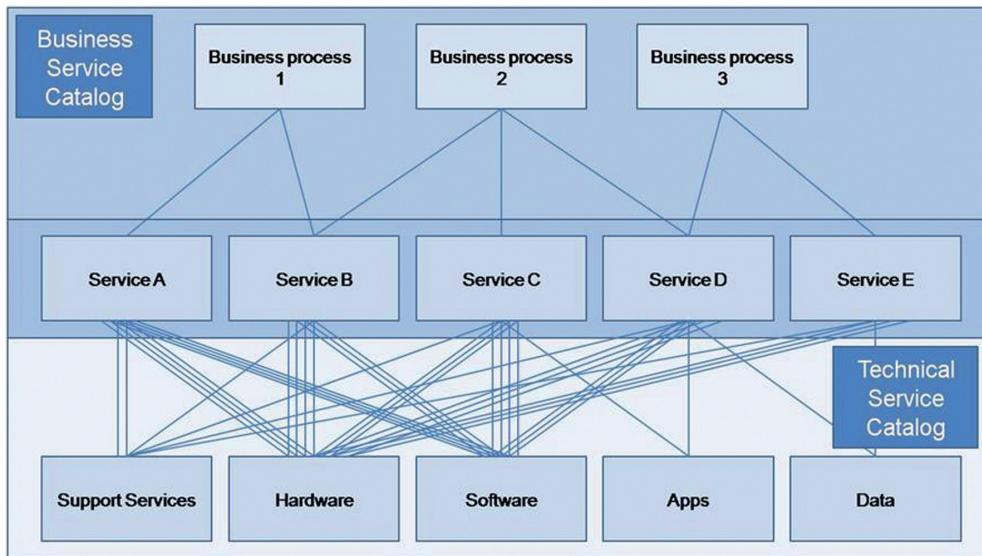


Figure 5.J—The Business and Technical Service Catalogs

© Crown Copyright 2011 Reproduced under license from OGC

Business Service Catalog: contains details of all the IT services defined in the context of customers, together with relationships to the business units and the business process they support. This information is utilized to form the customer view of the Service Catalog, using appropriate communication (language, use of business terminology, not overly technical) to ensure its effectiveness. In cases where the customer is an IT organization themselves, the technical level of detail provided should be appropriately expanded.

Technical Service Catalog: also contains details of all the IT services delivered to the customer, but by comparison, the Technical Service Catalog includes records of the relationships that exist with other supporting services, shared services, components, and Configuration Items necessary for the delivery of the service to the business. The Technical Service Catalog should underpin the Business Service Catalog and is not always visible to customers and users, unless specifically requested. In many cases, the Technical Service Catalog is formed largely by the information contained within the Configuration Management System.

Developing the Service Catalog

WHILE MORE EXTRAVAGANT IMPLEMENTATIONS OF the Service Catalog delivered via extensive internet/intranet solutions will maintain both aspects in an integrated fashion, less mature organizations may choose to maintain these separately. Regardless of the implementation method, the key requirement is that the desired information is easily accessible by the authorized parties and communicated in a form that is appropriate for the audience.

The starting point for any Service Catalog journey is to begin identifying what actual services are being provided and who are the customers of these services. While it sounds simple enough, for an organization with a long history and large amount of customers, there will often be a lack of clarity in this regard, resulting in confusion and debate about what actually constitutes a service.

From an IT perspective, many staff will typically identify IT systems, such as software or applications, as being the service offered to customers. In other cases, the service will be seen to be composed of multiple services (which in turn are formed by one or more IT systems). In short, looking at services from only an IT perspective will lead you down a dangerous path and most likely cause you more headaches and grief in the process.

Instead, the recommended starting point is to look at things from the customer perspective. This is normally performed by asking customers what they perceive to be the IT services they are utilizing and how they map onto and support their business processes. Just like the design of services should be coordinated in a top-down approach, so should the associated definition for inclusion in the Service Catalog. Regardless of exactly how this occurs, each organization needs to develop a policy defining what constitutes a service and how it is defined and agreed within their own organization.

The top-down approach may lead to the creation of a service hierarchy, qualifying types of services such as:

- **Business Services**—what is actually used and seen by the customer
- **Supporting Services**, including further definition as:
 - Infrastructure Services
 - Application Services
 - Network Services
 - Data Management Services

- **Shared and Commodity Services**
- **Externally provided Services**—those provided/managed by a 3rd party organization

As the definition of services begins to occur, consideration should be made as to who the actual customers of these services are. Eventually, through a cycle of discussions with customers, a clearer picture will emerge, providing the beginnings of a Business Service Catalog.

Inputs

A NUMBER OF SOURCES OF information are relevant to the Service Catalog Management process. These include:

- Business information from the organization's business and IT strategy, plans and financial plans, and information on their current and future requirements from the Service Portfolio
- BIA, providing information on the impact, priority, and risk associated with each service or changes to service requirements
- Business requirements, including details of any agreed, new, or changed business requirements from the Service Portfolio
- The Service Portfolio and all related data and documents
- The CMS
- RFCs
- Feedback from all other processes

Outputs

THE PROCESS OUTPUTS OF THE Service Catalog Management process are:

- The documentation and agreement of a definition of the service
- Updates to the service portfolio—should contain the current status of all services and requirements for services
- Updates to RFCs
- The Service Catalog—should contain the details and the current status of every live service provided by the service provider or service being transitioned into the live environment, together with the interfaces and dependencies

Capacity Management

Terminology

Term	Definition
application sizing	(<i>ITIL® Service Design</i>) The activity responsible for understanding the resource requirements needed to support a new application or a major change to an existing application. Application sizing helps to ensure that the IT service can meet its agreed service level targets for capacity and performance.
capacity	(<i>ITIL® Service Design</i>) The maximum throughput that a configuration item or IT service can deliver. For some types of CIs, capacity may be the size or volume—for example, a disk drive.
capacity management information system (CMIS)	(<i>ITIL® Service Design</i>) A set of tools, data, and information that is used to support capacity management.
capacity planning	See <i>also</i> service knowledge management system.
modeling	A technique that is used to predict the future behavior of a system, process, IT service, configuration item, etc. Modeling is commonly used in financial management, capacity management, and availability management.
service capacity management (SCM)	(<i>ITIL® Continual Service Improvement</i>) (<i>ITIL® Service Design</i>) The sub-process of capacity management responsible for understanding the performance and capacity of IT services. Information on the resources used by each IT service and the pattern of usage over time are collected, recorded, and analyzed for use in the capacity plan.
tuning	The activity responsible for planning changes to make the most efficient use of resources. Tuning is most commonly used in the context of IT services and components. Tuning is part of capacity management, which also includes performance monitoring and implementation of the required changes. Tuning is also called optimization, particularly in the context of processes and other nontechnical resources.

Purpose

THE PURPOSE OF THE CAPACITY Management process is to ensure that the capacity of IT services and the IT infrastructure meets the agreed capacity- and performance-related requirements in a cost-effective and timely manner. Capacity Management is concerned with meeting both the current and future capacity and performance needs of the business.

The objectives of capacity management are to:

- Produce and maintain an appropriate and up-to-date capacity plan, which reflects the current and future needs of the business
- Provide advice and guidance to all other areas of the business and IT on all capacity- and performance-related issues
- Ensure that service performance achievements meet all of their agreed targets by managing the performance and capacity of both services and resources
- Assist with the diagnosis and resolution of performance- and capacity-related incidents and problems
- Assess the impact of all changes on the capacity plan and the performance and capacity of all services and resources
- Ensure that proactive measures to improve the performance of services are implemented wherever it is cost-justifiable to do so

Scope

CAPACITY MANAGEMENT PROVIDES THE PREDICTIVE and ongoing capacity indicators needed to align capacity to demand. It is about finding the right balance between resources and capabilities and demand.



Figure 5.K—The Balancing Act of Capacity Management

IN COORDINATION WITH THE PROCESSES found in the Service Strategy stage, Capacity Management seeks to provide a continual optimal balance between supply against demand and costs against resources needed.

This optimum balance is only achieved both now and in the future by ensuring that Capacity Management is involved in all aspects of the Service Lifecycle. When this doesn't occur, Capacity Management only operates as a reactive process with limited benefits being delivered as a result.

The Capacity Management process should be the focal point for all IT performance and capacity issues. Capacity Management considers all resources required to deliver the IT service and plans for short-, medium-, and long-term business requirements.

The Capacity Management process should include:

- Monitoring patterns of business activity through performance, utilization, and throughput of IT services and the supporting infrastructure, environmental, data, and applications components and the production of regular and ad hoc reports on service and component capacity and performance
- Undertaking tuning activities to make the most efficient use of existing IT resources
- Understanding the agreed current and future demands being made by the customer for IT resources and producing forecasts for future requirements
- Influencing demand in conjunction with the Financial Management for IT services and Demand Management processes
- Producing a capacity plan that enables the service provider to continue to provide services of the quality defined in SLAs and that covers a sufficient planning timeframe to meet future service levels required as defined in the Service Portfolio and SLRs
- Assisting with the identification and resolution of any incidents and problems associated with service or component capacity or performance
- The proactive improvement of service or component performance, wherever it is cost-justifiable and meets the needs of the business

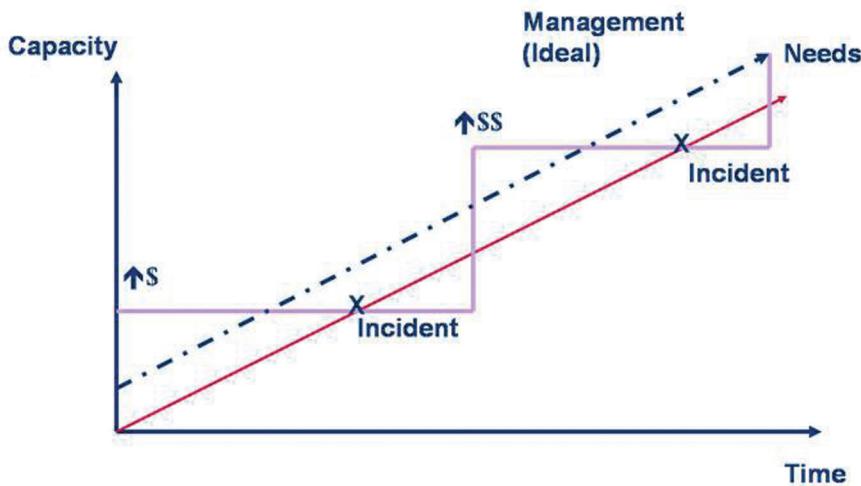


Figure 5.1—Capacity Management When Used Reactively

IN THE ABOVE FIGURE, CAPACITY is only implemented when disruptions begin to occur as demand has exceeded supply. While the implemented capacity does work to resolve the disruptions, there are some consequences to this type of reactive behavior including:

- IT infrastructure components being purchased that do not optimally fit the requirements or architecture
- Budget overruns for the unforeseen and unanticipated purchases
- Periods of time where there are potentially large amounts of excess capacity
- Reduced customer and user satisfaction with the affected IT services
- A general negatively affected perception of the IT organization as a whole

Sub-Processes of Capacity Management:

SOME OF THE ACTIVITIES OF Capacity Management are defined in the context of three sub-processes, consisting of Business, Service, and Component Capacity Management. Besides these, there will also be discussion of the operational activities required as well as the techniques that are utilized in various forms by the three different sub - processes.

Business Capacity Management:

- Manages Capacity to meet future business requirements for IT services
- Identifies changes occurring in the business to assess how they might impact capacity and performance of IT services
- Plans and implements sufficient capacity in an appropriate timescale
- Should be included in Change Management and Project Management activities

Service Capacity Management

- Focuses on managing ongoing service performance as detailed in the Service Level Agreements
- Establishes baselines and profiles of use of services, including all components and sub-services that affect the user experience
- Reports to the Service Level Manager and Service Owner regarding end-to-end service capacity, performance, and utilization

Component Capacity Management

- Identifies and manages each of the individual components of the IT Infrastructure (e.g., CPU, memory, disks, network bandwidth, server load)
- Evaluates new technology and how it might be leveraged to benefit the organization
- Balances loads across resources for optimal performance of services

All three sub-processes collate their data for use by other ITSM processes, primarily Service Level Management and Financial Management.

Activities

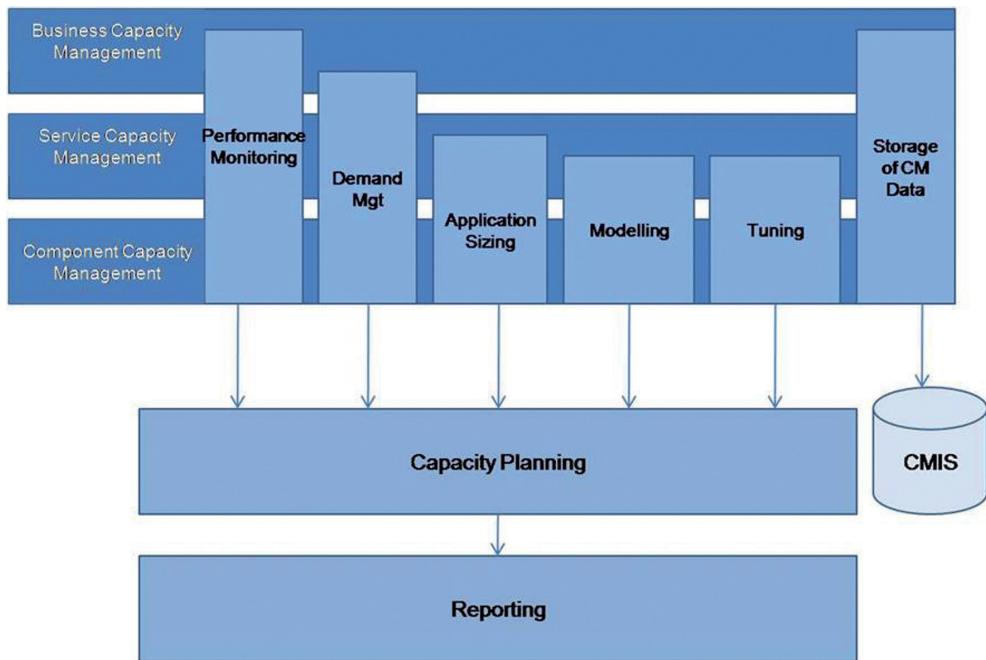


Figure 5.M—Activities of Capacity Management

© Crown Copyright 2011 Reproduced under license from OGC

Capacity Management consists of these main activities:

- **Performance Monitoring:** measuring, monitoring, and tuning the performance of IT services and the individual infrastructure components
- **Demand Management:** short term reactive implementation of strategies considered within Service Strategy to manage current demand
- **Application Sizing:** determining the hardware or application capacity required to support new or modified applications and their predicted workload
- **Modeling:** used to forecast the behavior of the infrastructure under *certain conditions* (e.g., *what if the number of users doubled?*; *what if a network segment fails?*)
- **Tuning:** modifications made under the control of Change Management to enable better utilization of current infrastructure

- **Storage of Capacity Management Data:** storing all business, service, and component capacity data to assist decision-making within the Capacity Management and Financial Management processes
- **Capacity Planning:** forecasting when and where capacity will need to be increased and decreased. A formal Capacity Plan will document these recommendations
- **Reporting**

Roles and Responsibilities

Capacity Manager

- Responsibilities:
 - Ensure adequate performance and capacity for all IT services
 - Capacity Plan (responsible for its development and management)
 - Delegate responsibility for performance and capacity monitoring and alerting tasks
 - Report provision and advice to other areas of IT and the business
- Skills: Strategic business awareness, technical, analytical, consultancy

Capacity Management is critical for ensuring effective and efficient capacity and performance of IT Services and IT components in line with identified business requirements and the overall IT strategic objectives. It is essential that the Capacity Manager ensures that the process is appropriately integrated with all aspects of the Service Lifecycle.

Inputs

A NUMBER OF SOURCES OF information are relevant to the Capacity Management process. Some of these are as follows.

- **Business information:** from the organization's business strategy, plans and financial plans, and information on their current and future requirements
- **Service and IT information:** from Service Strategy, the IT strategy and plans and current budgets, covering all areas of technology and technology plans, including the infrastructure, environment, data,

and applications and the way in which they relate to business strategy and plans

- **Component performance and capacity information:** of both existing and new technology from manufacturers and suppliers
- **Service performance issue information:** the Incident and Problem Management processes, with incidents and problems relating to poor performance
- **Service information:** from the SLM process with details of the services from the Service Portfolio, the Service Catalog, and service level targets within SLAs and SLRs and possibly from the monitoring of SLAs, service reviews, and breaches of the SLAs
- **Financial information:** from Financial Management for IT services, the cost of service provision, the cost of resources, components and upgrades, the resultant business benefit, and the financial plans and budgets, together with the costs associated with service and component failure. Some of the costs of components and upgrades to components will be obtained from procurement, suppliers, and manufacturers
- **Change information:** from the Change Management process, with a change schedule and a need to assess all changes for their impact on the capacity of the technology
- **Performance information:** from the CMIS on the current performance of both all existing services and IT infrastructure components
- **CMS:** containing information on the relationships between the business, the services, the supporting services, and the technology
- **Workload information:** from the IT operations team, with schedules of all the work that needs to be run and information on the dependencies between different services and information and the interdependencies within a service

Outputs

THE OUTPUTS OF CAPACITY MANAGEMENT are:

- **CMIS:** this holds the information needed by all sub-processes within Capacity Management. For example, the data monitored and collected as part of Component and Service Capacity Management is used in Business Capacity Management to determine what infrastructure components or upgrades to components are needed and when.
- **Capacity plan:** this is used by all areas of the business and IT management and is acted on by the IT service provider and senior

management of the organization to plan the capacity of the IT infrastructure. It contains information on the current usage of service and components and plans for the development of IT capacity to meet the needs in the growth of both existing services and any agreed new services. The capacity plan should be actively used as a basis for decision-making.

- **Service performance information and reports:** This is used by many other processes. For example, the Capacity Management process assists SLM with the reporting and reviewing of service performance and the development of new SLRs or changes to existing SLAs. It also assists the Financial Management for IT services process by identifying when money needs to be budgeted for IT infrastructure upgrades or the purchase of new components.
- **Workload analysis and reports:** this is used by IT operations to assess and implement changes in conjunction with Capacity Management to schedule or reschedule when services or workloads are run to ensure that the most effective and efficient use is made of the available resources
- **Ad hoc capacity and performance reports:** these are used by all areas of Capacity Management, IT, and the business to analyze and resolve service and performance issues
- **Forecasts and predictive reports:** these are used by all areas to analyze, predict, and forecast particular business and IT scenarios and their potential solutions
- **Thresholds, alerts, and events**
- **Improvement actions:** for inclusion in an SIP

Availability Management

Terminology

Term	Definition
availability	(<i>ITIL® Service Design</i>) Ability of an IT service or other configuration item to perform its agreed function when required. Availability is determined by reliability, maintainability, serviceability, performance, and security. Availability is usually calculated as a percentage. This calculation is often based on agreed service time and downtime. It is best practice to calculate availability of an IT service using measurements of the business output.
availability management information system (AMIS)	(<i>ITIL® Service Design</i>) A set of tools, data, and information that is used to support availability management. See also service knowledge management system.
downtime	(<i>ITIL® Service Design</i>) (<i>ITIL® Service Operation</i>) The time when an IT service or other configuration item is not available during its agreed service time. The availability of an IT service is often calculated from agreed service time and downtime.
maintainability	(<i>ITIL® Service Design</i>) A measure of how quickly and effectively an IT service or other configuration item can be restored to normal working after a failure. Maintainability is often measured and reported as MTRS. Maintainability is also used in the context of software or IT service development to mean ability to be changed or repaired easily.
reliability	(<i>ITIL® Continual Service Improvement</i>) (<i>ITIL® Service Design</i>) A measure of how long an IT service or other configuration item can perform its agreed function without interruption. Usually measured as MTBF or MTBSI. The term can also be used to state how likely it is that a process, function, etc. will deliver its required outputs. See also availability.
resilience	(<i>ITIL® Service Design</i>) The ability of an IT service or other configuration item to resist failure or to recover in a timely manner following a failure. For example, an armored cable will resist failure when put under stress.
response time	A measure of the time taken to complete an operation or transaction. Used in capacity management as a measure of IT infrastructure performance and in incident management as a measure of the time taken to answer the phone or to start diagnosis.

Term	Definition
risk	A possible event that could cause harm or loss or affect the ability to achieve objectives. A risk is measured by the probability of a threat, the vulnerability of the asset to that threat, and the impact it would have if it occurred. Risk can also be defined as uncertainty of outcome and can be used in the context of measuring the probability of positive outcomes as well as negative outcomes.
risk assessment	The initial steps of risk management: analyzing the value of assets to the business, identifying threats to those assets, and evaluating how vulnerable each asset is to those threats. Risk assessment can be quantitative (based on numerical data) or qualitative.
risk management	The process responsible for identifying, assessing, and controlling risks. Risk management is also sometimes used to refer to the second part of the overall process after risks have been identified and assessed, as in 'risk assessment and management'. This process is not described in detail within the core ITIL® publications.
	See also risk assessment.
serviceability	<i>(ITIL® Continual Service Improvement)</i> <i>(ITIL® Service Design)</i> The ability of a third-party supplier to meet the terms of its contract. This contract will include agreed levels of reliability, maintainability, and availability for a configuration item.
trend analysis	<i>(ITIL® Continual Service Improvement)</i> Analysis of data to identify time-related patterns. Trend analysis is used in problem management to identify common failures or fragile configuration items and in capacity management as a modeling tool to predict future behavior. It is also used as a management tool for identifying deficiencies in IT service management processes.
vital business function (VBF)	<i>(ITIL® Service Design)</i> Part of a business process that is critical to the success of the business. Vital business functions are an important consideration of business continuity management, IT service continuity management, and availability management.
vulnerability	A weakness that could be exploited by a threat—for example, an open firewall port, a password that is never changed, or a flammable carpet. A missing control is also considered to be a vulnerability.

Purpose

AVAILABILITY IS ONE OF THE most critical parts of the warranty of a service. If a service does not deliver the levels of availability required, then the business will not experience the value that has been promised. Without availability, the utility of the service cannot be accessed. Availability Management process activity extends across the service lifecycle.

The purpose of the Availability Management process is to ensure that the level of availability delivered in all IT services meets the agreed availability needs and/or service level targets in a cost-effective and timely manner. Availability Management is concerned with meeting both the current and future availability needs of the business.

Availability Management defines, analyzes, plans, measures, and improves all aspects of the availability of IT services, ensuring that all IT infrastructure, processes, tools, roles etc. are appropriate for the agreed availability service level targets. It provides a point of focus and management for all availability-related issues, relating to both services and resources, ensuring that availability targets in all areas are measured and achieved.

The objectives of Availability Management are to:

- Produce and maintain an appropriate and up-to-date availability plan that reflects the current and future needs of the business
- Provide advice and guidance to all other areas of the business and IT on all availability-related issues
- Ensure that service availability achievements meet all their agreed targets by managing services and resources-related availability performance
- Assist with the diagnosis and resolution of availability-related incidents and problems
- Assess the impact of all changes on the availability plan and the availability of all services and resources
- Ensure that proactive measures to improve the availability of services are implemented wherever it is cost-justifiable to do so.

Question:

Why could users be happy with a 60 minute outage and yet be unhappy with 30 minute outage?

1. 30min outage during peak time, overtime being paid to staff, urgent report required
2. 60min outage on weekend, holiday, off peak, when service not required
3. 30min outage on critical IT Service, 60min outage on non-critical IT Service
4. 30mins unplanned outage, 60min planned outage (e.g., maintenance)

For a consumer/user of an IT service, its availability and reliability can directly influence both the perception and satisfaction of the overall IT service provision. However, when disruptions are properly communicated and managed effectively, the impact on the user population's experience can be significantly reduced.

Scope

THE SCOPE OF THE AVAILABILITY Management process covers the design, implementation, measurement, management, and improvement of IT service and component availability. Availability Management commences as soon as the availability requirements for an IT service are clear enough to be articulated. It is an ongoing process, finishing only when the IT service is decommissioned or retired.

The Availability Management process includes two key elements:

- **Reactive activities:** these involve the monitoring, measuring, analysis, and management of all events, incidents, and problems involving unavailability. These activities are principally performed as part of the operational roles.
- **Proactive activities:** these involve the proactive planning, design, and improvement of availability. These activities are principally performed as part of the design and planning roles.

Availability Management needs to understand the service and component availability requirements from the business perspective, in terms of the:

- Current business processes, their operation, and requirements
- Future business plans and requirements
- Service targets and the current IT service operation and delivery
- IT infrastructure, data, applications, environment, and their performance
- Business impacts and priorities in relation to the services and their usage

Understanding all of this will enable Availability Management to ensure that all the services and components are designed and delivered to meet their targets in terms of agreed business needs.

The Availability Management process:

- Should be applied to all operational services and technology, particularly those covered by SLAs. It can also be applied to those IT services deemed to be business-critical, regardless of whether formal SLAs exist.
- Should be applied to all new IT services and for existing services where SLRs or SLAs have been established
- Should be applied to all supporting services and the partners and suppliers (both internal and external) that form the IT support organization as a precursor to the creation of formal agreements
- Should consider all aspects of the IT services and components and supporting organizations that may impact availability, including training, skills, process effectiveness, procedures, and tools.

The Availability Management process should include:

- Monitoring of all aspects of availability, reliability, and maintainability of IT services and the supporting components with appropriate events, alarms, and escalation, with automated scripts for recovery
- Maintaining a set of methods, techniques, and calculations for all availability measurements, metrics, and reporting
- Actively participating in risk assessment and management activities
- Collecting measurements and the analysis and production of regular and ad hoc reports on service and component availability

- Understanding the agreed current and future demands of the business for IT services and their availability
- Influencing the design of services and components to align with business availability needs
- Producing an availability plan that enables the service provider to continue to provide and improve services in line with availability targets defined in SLAs and to plan and forecast future availability levels required, as defined in SLRs
- Maintaining a schedule of tests for all resilience and fail-over components and mechanisms
- Assisting with the identification and resolution of any incidents and problems associated with service or component unavailability
- Proactively improving service or component availability wherever it is cost-justifiable and meets the needs of the business.

The Availability Management process does not include Business Continuity Management (BCM) and the resumption of business processing after a major disaster. The support of BCM is included within ITSCM. However, Availability Management does provide key inputs to ITSCM and the two processes have a close relationship, particularly in the assessment and management of risks and in the implementation of risk reduction and resilience measures.

Activities

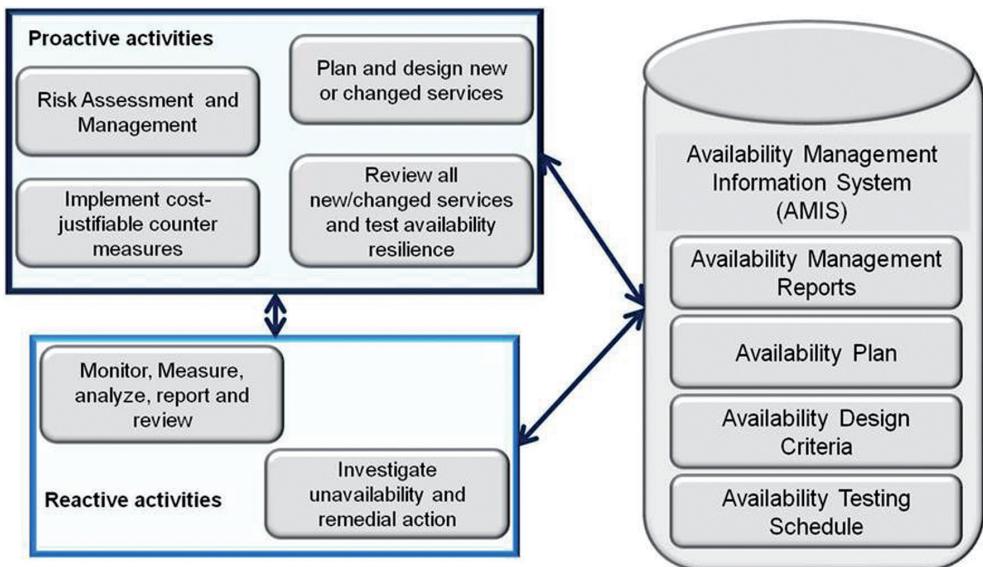


Figure 5.N—The Proactive and Reactive Elements of Availability Management
 © Crown Copyright 2011 Reproduced under license from OGC

- **Proactive Activities (primarily executed in Service Design and Service Transition):**
 - The development and maintenance of an availability plan, which documents the current and future requirements for service availability and the methods used to meet these requirements
 - Development of a defined set of methods, techniques, and calculations for the assessment and reporting of availability
 - Liaison with IT Service Continuity Management and other aligned processes to assist with risk assessment and management activities
 - Ensuring consistency in the design of services and components to align with the business requirements for availability
- **Reactive Activities (primarily executed in Service Operation and Continual Service Improvement):**
 - Regular monitoring of all aspects of availability, reliability, and maintainability, including supporting processes such as Event Management for timely disruption detection and escalation

- › Regular and event-based reporting of service and component availability
- › Ensuring regular maintenance is performed according to the levels of risk across the IT infrastructure
- › Assessing the performance of and data gathered by various Service Operation processes, such as Incident and Problem Management, to determine what improvement actions might be made to improve availability levels or the way in which they are met.

Expanded Incident Lifecycle

AN AIM OF AVAILABILITY MANAGEMENT is to ensure the duration and impact from incidents impacting IT services are minimized to enable business operations to resume as quickly as possible.

The expanded incident lifecycle enables the total IT service downtime for any given incident to be broken down and mapped against the major stages that all incidents go through.

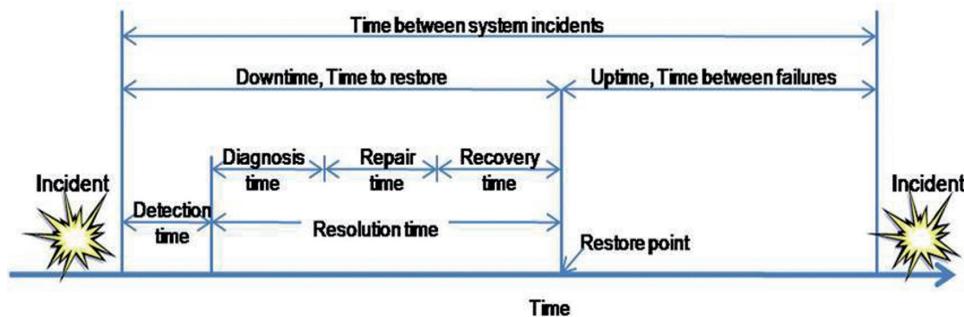


Figure 5.0—The Expanded Incident Lifecycle

© Crown Copyright 2011 Reproduced under license from OGC

- **Mean Time Between Failures (MTBF) or Uptime:**
 - Average time between the recovery from one incident and the occurrence of the next incident, relates to the reliability of the service
- **Mean Time to Restore Service (MTRS) or Downtime:**
 - Average time taken to restore a CI or IT service after a failure
 - Measured from when CI or IT service fails until it is fully restored and delivering its normal functionality
- **Mean Time Between System Incidents (MTBSI):**
 - Average time between the occurrences of two consecutive incidents
 - Sum of the MTRS and MTBF
- **Relationships of the above terms:**
 - High ratio of MTBF/MTBSI indicates there are frequently occurring minor faults or disruptions
 - Low ratio of MTBF/MTBSI indicates there are infrequently occurring major faults or disruptions

Elements making up the Mean Time to Restore Service (MTRS):

- **Detection Time:** Time for the service provider to be informed of the fault (reported)
- **Diagnosis Time:** Time for the service provider to respond after diagnosis completed
- **Repair Time:**
 - Time for the service provider to restore the components that caused the fault
 - Calculated from **diagnosis to recovery** time
- **Restoration Time (MTRS):**
 - The **agreed** level of service is restored to the user
 - Calculated from **detection to restore point**
- **Restore Point:** The point where the agreed level of service has been restored

Roles and Responsibilities

Availability Manager

- **Responsibilities:**
 - Ensure adequate availability of all IT services
 - Developing and maintaining an availability plan
 - Oversee availability monitoring and improvement of the process
 - Report provision and advice

Skills: Awareness of how IT supports the business, technical, analytical, consultancy, seeks continuous improvement

Note: The Availability Manager does not seek to achieve 100% availability of all services and systems but, instead, seeks to deliver availability that matches or exceeds (within reason) the agreed business requirements.

Availability Management Metrics

TYPICAL METRICS FOR EVALUATING THE effectiveness and efficiency of Availability Management include:

- Percentage reduction in unavailability of services and components
- Percentage increase in the reliability of services and components
- Effective review and follow up of all SLA, OLA, and UC breaches
- Percentage improvement in overall end-to-end availability of service
- Percentage reduction in the number and impact of service breaks
- Improvement of MTBF
- Improvement of MTBSI
- Reduction in MTRS

While the above list does include a number of important measures, the service provider should also seek to demonstrate the impact that availability/unavailability has on the business. Such examples of business-oriented availability reporting include:

- User minutes lost due to disruption
- Transactions lost or delayed due to disruption
- Customer complaints caused by disruption

Inputs

A NUMBER OF SOURCES OF information are relevant to the Availability Management process. Some of these are as follows:

- **Business information:** from the organization's business strategy, plans and financial plans, and information on their current and future requirements, including the availability requirements for new or enhanced IT services
- **Business impact information:** from BIAs and assessment of VBFs underpinned by IT services
- **Reports and registers:** previous risk assessment reports and a risk register
- **Service information:** from the Service Portfolio and the Service Catalog
- **Service information:** from the SLM process, with details of the services from the Service Portfolio and the Service Catalog, service level targets within SLAs and SLRs, service reviews and breaches of the SLAs
- **Financial information:** from Financial Management for IT services, the cost of service provision, the cost of resources and components
- **Change and release information:** from the Change Management process, with a change schedule, the release schedule from release and deployment management, and a need to assess all changes for their impact on service availability
- **Service asset and configuration management:** containing information on the relationships between the business, the services, the supporting services, and the technology
- **Service targets:** from SLAs, SLRs, OLAs, and contracts
- **Component information:** on the availability, reliability, and maintainability requirements for the technology components that underpin IT service(s)
- **Technology information:** from the CMS on the topology and the relationships between the components and the assessment of the capabilities of new technology
- **Past performance:** from previous measurements, achievements, and reports and the Availability Management Information System (AMIS)
- **Unavailability and failure information:** from incidents and problems
- **Planning information:** from other processes, such as the capacity plan from Capacity Management

Outputs

THE OUTPUTS PRODUCED BY AVAILABILITY Management should include:

- The Availability MIS (AMIS)
- The availability plan for the proactive improvement of IT services and technology
- Availability and recovery design criteria and proposed service targets for new or changed services
- Service availability, reliability, and maintainability reports of achievements against targets, including input for all service reports
- Component availability, reliability, and maintainability reports of achievements against targets
- Revised risk assessment reviews and reports and an updated risk register
- Monitoring, management, and reporting requirements for IT services and components to ensure that deviations in availability, reliability, and maintainability are detected, actioned, recorded, and reported
- An availability management test schedule for testing all availability, resilience, and recovery mechanisms
- The planned and preventive maintenance schedules
- Contributions for the PSO to be created by change in collaboration with Release and Deployment Management
- Details of the proactive availability techniques and measures that will be deployed to provide additional resilience to prevent or minimize the impact of component failures on the IT service availability
- Improvement actions for inclusion within the SIP

IT Service Continuity Management

SERVICE CONTINUITY IS AN ESSENTIAL part of the warranty of a service. If a service's continuity cannot be maintained and/or restored in accordance with the requirements of the business, then the business will not experience the value that has been promised. Without continuity the utility of the service cannot be accessed.

The purpose of the IT Service Continuity Management (ITSCM) process is to support the overall Business Continuity Management (BCM) process by ensuring that the IT service provider can always provide minimum agreed business continuity-related service levels by managing the risks that could seriously affect IT services.

In support of and alignment with the BCM process, ITSCM uses formal risk assessment and management techniques to:

- Reduce risks to IT services to agreed acceptable levels
- Plan and prepare for the recovery of IT services

The objectives of ITSCM are to:

- Produce and maintain a set of IT service continuity plans that support the overall business continuity plans of the organization
- Complete regular BIA exercises to ensure that all continuity plans are maintained in line with changing business impacts and requirements
- Conduct regular risk assessment and management exercises to manage IT services within an agreed level of business risk in conjunction with the business and the Availability Management and Information Security Management processes
- Provide advice and guidance to all other areas of the business and IT on all continuity-related issues
- Ensure that appropriate continuity mechanisms are put in place to meet or exceed the agreed business continuity targets
- Assess the impact of all changes on the IT service continuity plans and supporting methods and procedures
- Ensure that proactive measures to improve the availability of services are implemented wherever it is cost-justifiable to do so
- Negotiate and agree contracts with suppliers for the provision of the necessary recovery capability to support all continuity plans in conjunction with the Supplier Management process

Note: ITSCM is often referred to as Disaster Recovery planning.

Terminology

Term	Definition
business continuity plan (BCP)	(ITIL® Service Design) A plan defining the steps required to restore business processes following a disruption. The plan also identifies the triggers for invocation, people to be involved, communications, etc. IT service continuity plans form a significant part of business continuity plans.
business impact analysis (BIA)	(ITIL® Service Strategy) Business impact analysis is the activity in business continuity management that identifies vital business functions and their dependencies. These dependencies may include suppliers, people, other business processes, IT services etc. Business impact analysis defines the recovery requirements for IT services. These requirements include recovery time objectives, recovery point objectives, and minimum service level targets for each IT service.
countermeasure	Can be used to refer to any type of control. The term is most often used when referring to measures that increase resilience, fault tolerance, or reliability of an IT service.
gradual recovery	(ITIL® Service Design) A recovery option that is also known as cold standby. Gradual recovery typically uses a portable or fixed facility that has environmental support and network cabling but no computer systems. The hardware and software are installed as part of the IT service continuity plan. Gradual recovery typically takes more than three days and may take significantly longer.
hot standby	See fast recovery; immediate recovery.
immediate recovery	(ITIL® Service Design) A recovery option that is also known as hot standby. Provision is made to recover the IT service with no significant loss of service to the customer. Immediate recovery typically uses mirroring, load balancing, and split-site technologies.
impact	(ITIL® Service Operation) (ITIL® Service Transition) A measure of the effect of an incident, problem, or change on business processes. Impact is often based on how service levels will be affected. Impact and urgency are used to assign priority.
intermediate recovery	(ITIL® Service Design) A recovery option that is also known as warm standby. Intermediate recovery usually uses a shared portable or fixed facility that has computer systems and network components. The hardware and software will need to be configured and data will need to be restored as part of the IT service continuity plan. Typical recovery times for intermediate recovery are one to three days.

Term	Definition
IT service continuity plan	(ITIL® Service Design) A plan defining the steps required to recover one or more IT services. The plan also identifies the triggers for invocation, people to be involved, communications, etc. The IT service continuity plan should be part of a business continuity plan.
manual workaround	(ITIL® Continual Service Improvement) A workaround that requires manual intervention. Manual workaround is also used as the name of a recovery option in which the business process operates without the use of IT services. This is a temporary measure and is usually combined with another recovery option.
reciprocal arrangement	(ITIL® Service Design) A recovery option. An agreement between two organizations to share resources in an emergency—for example, high-speed printing facilities or computer room space.
risk	A possible event that could cause harm or loss or affect the ability to achieve objectives. A risk is measured by the probability of a threat, the vulnerability of the asset to that threat, and the impact it would have if it occurred. Risk can also be defined as uncertainty of outcome and can be used in the context of measuring the probability of positive outcomes as well as negative outcomes.
risk assessment	The initial steps of risk management: analyzing the value of assets to the business, identifying threats to those assets, and evaluating how vulnerable each asset is to those threats. Risk assessment can be quantitative (based on numerical data) or qualitative.
risk management	The process responsible for identifying, assessing, and controlling risks. Risk management is also sometimes used to refer to the second part of the overall process after risks have been identified and assessed, as in 'risk assessment and management'. This process is not described in detail within the core ITIL® publications.
threat	See also risk assessment. A threat is anything that might exploit a vulnerability. Any potential cause of an incident can be considered a threat. For example, a fire is a threat that could exploit the vulnerability of flammable floor coverings. This term is commonly used in information security management and IT service continuity management but also applies to other areas, such as problem and availability management.
vital business function (VBF)	(ITIL® Service Design) Part of a business process that is critical to the success of the business. Vital business functions are an important consideration of business continuity management, IT service continuity management, and availability management.

Term	Definition
vulnerability	A weakness that could be exploited by a threat—for example, an open firewall port, a password that is never changed, or a flammable carpet. A missing control is also considered to be a vulnerability.
warm standby	See intermediate recovery.

Scope

THE SCOPE OF ITSCM CAN be said to be focused on planning for, managing, and recovering from IT disasters. These disasters are severe enough to have a critical impact on business operations and, as a result, will typically require a separate set of infrastructure and facilities to recover. Less significant events are dealt with as part of the Incident Management process in association with Availability Management.

The disaster does not necessarily need to be a fire, flood, pestilence, or plague; it can any disruption that causes a severe impact to one or more business processes. Accordingly, the scope of ITSCM should be carefully defined according to the organization's needs, which may result in continuity planning and recovery mechanisms for some or all of the IT services being provided to the business.

There are longer-term business risks that are out of the scope of ITSCM, including those arising from changes in business direction, organizational restructures, or emergence of new competitors in the market place. These are more the focus of processes such as Service Portfolio Management and Change Management.

The ITSCM process includes:

- The agreement of the scope of the ITSCM process and the policies adopted
- BIA to quantify the impact loss of IT service would have on the business
- Risk assessment and management—the risk identification and risk assessment to identify potential threats to continuity and the likelihood of the threats becoming reality. This also includes taking measures to manage the identified threats where this can be cost-justified. The approach to managing these threats will form the core of the ITSCM strategy and plans.
- Production of an overall ITSCM strategy that must be integrated into the BCM strategy. This can be produced following the two steps identified above and is likely to include elements of risk reduction as well as selection of appropriate and comprehensive recovery options.
- Production of an ITSCM plan, which again must be integrated with the overall BCM plans
- Testing of the plans
- Ongoing operation and maintenance of the plans

Activities of IT Service Continuity Management

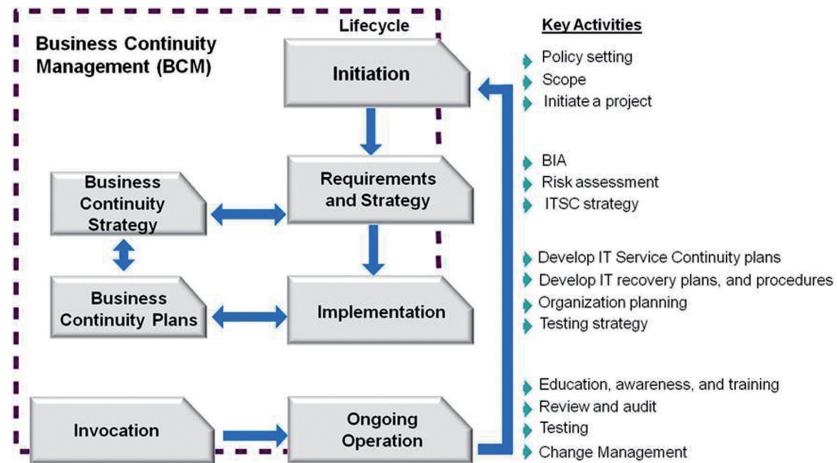


Figure 5.P—Activities of IT Service Continuity Management

© Crown Copyright 2011 Reproduced under license from OGC

Performing a Business Impact Analysis (BIA) identifies:

- Critical business processes and Vital Business Functions
- Potential damage or loss caused by disruption
- Possible escalations caused by damage or loss
- Necessary resources required to enable continuity of critical business processes
- Time constraints for minimum recovery of facilities and services
- Time constraints for complete recovery of facilities and services

Risk Assessment:

- Gather information on assets (IT infrastructure components)
- Threats from both internal and external sources (the likelihood of occurring)
- Vulnerabilities (the extent of impact or effect on organization)

Ongoing Operation

- Education and awareness
 - Involving IT staff, customers, users, suppliers, and other stakeholders
- Training
- Reviews
- Ongoing testing
 - At least annually
 - Following major changes
- Audits of recovery procedures, risk-reduction measures, and for compliance to procedures.
- Ensuring integration with Change Management so that all changes are assessed as to their requirements for continuity and their potential impact on existing continuity strategies

Roles and Responsibilities

TYPICAL RESPONSIBILITIES FOR **ITSCM** IN planning and dealing with disasters are similar to how First Aid Officers and Fire Wardens act in planning and operational roles (they may not be full-time roles but are, instead, a ‘hat’ they wear when required). See the following table for an example of how responsibilities for ITSCM are typically assigned.

Role	Responsibilities
Board	Crisis management Corporate/business decisions External affairs
Senior Management	Co-ordination Direction and arbitration Resource authorization
Management	Invocation of continuity or recovery Team leadership Site management Liaison and reporting
Supervisors and Staff	Task execution Team membership Team and site liaison

Skill requirements for the ITSCM Manager and other involved staff include:

- Knowledge of the business (help to set priorities for protection and recovery)
- Calm under pressure
- Analytical (problem solving)
- Leadership and team players
- Negotiation and communication

Inputs

THERE ARE MANY SOURCES OF input required by the ITSCM process:

- **Business information:** from the organization's business strategy, plans and financial plans, and information on their current and future requirements
- **IT information: from the IT strategy and plans and current budgets**
- **A business continuity strategy** and a set of business continuity plans: from all areas of the business
- **Service information:** from the SLM process, with details of the services from the Service Portfolio and the Service Catalog and service level targets within SLAs and SLRs
- **Financial information:** from Financial Management for IT services, the cost of service provision, the cost of resources and components
- **Change information:** from the Change Management process, with a change schedule and a need to assess all changes for their impact on all ITSCM plans
- **CMS:** containing information on the relationships between the business, the services, the supporting services, and the technology
- **Business Continuity Management** and Availability Management testing schedules
- **Capacity Management information:** identifying the resources required to run the critical services in the event of a continuity event
- **IT service continuity plans and test reports:** from supplier and partners, where appropriate

Outputs

THE OUTPUTS FROM THE ITSCM process include:

- A revised ITSCM policy and strategy
- **A set of ITSCM plans:** including all crisis management plans, emergency response plans, and disaster recovery plans, together with a set of supporting plans and contracts with recovery service providers
- **BIA exercises and reports:** in conjunction with BCM and the business
- **Risk assessment and management reviews and reports:** in conjunction with the business, Availability Management, and Information Security Management
- An ITSCM testing schedule
- ITSCM test scenarios
- ITSCM test reports and reviews

Forecasts and predictive reports are used by all areas to analyze, predict, and forecast particular business and IT scenarios and their potential solutions.

Information Security Management

Purpose

INFORMATION SECURITY IS A MANAGEMENT process within the corporate governance framework, which provides the strategic direction for security activities and ensures objectives are achieved. It further ensures that the information security risks are appropriately managed and that enterprise information resources are used responsibly. Information Security Management provides a focus for all aspects of IT security and manages all IT security activities.

In this context, the term 'information' is used as a general term and includes data stores, databases, and metadata.

Information security is a critical part of the warranty of a service. If the security of a service's information and information processing cannot be maintained at the levels required by the business, then the business will not experience the value that has been promised. Without information security, the utility of the service cannot be accessed.

The purpose of the Information Security Management process is to align IT security with business security and ensure that the confidentiality, integrity, and availability of the organization's assets, information, data, and IT services always matches the agreed needs of the business.

The objective of Information Security Management is to protect the interests of those relying on information and the systems and communications that deliver the information from harm resulting from failures of confidentiality, integrity, and availability.

For most organizations, the security objective is met when:

- Information is observed by or disclosed to only those who have a right to know (confidentiality)
- Information is complete, accurate, and protected against unauthorized modification (integrity)
- Information is available and usable when required, and the systems that provide it can appropriately resist attacks and recover from or prevent failures (availability)
- Business transactions, as well as information exchanges between enterprises or with partners, can be trusted (authenticity and non-repudiation)

Terminology

Term	Definition
confidentiality	(ITIL® Service Design) A security principle that requires that data should only be accessed by authorized people.
information security policy	(ITIL® Service Design) The policy that governs the organization's approach to information security management.
risk	A possible event that could cause harm or loss or affect the ability to achieve objectives. A risk is measured by the probability of a threat, the vulnerability of the asset to that threat, and the impact it would have if it occurred. Risk can also be defined as uncertainty of outcome and can be used in the context of measuring the probability of positive outcomes as well as negative outcomes.
risk assessment	The initial steps of risk management: analyzing the value of assets to the business, identifying threats to those assets, and evaluating how vulnerable each asset is to those threats. Risk assessment can be quantitative (based on numerical data) or qualitative.
risk management	The process responsible for identifying, assessing, and controlling risks. Risk management is also sometimes used to refer to the second part of the overall process after risks have been identified and assessed, as in 'risk assessment and management'. This process is not described in detail within the core ITIL® publications. See also risk assessment.
security	See information security management.
security management information system (SMIS)	(ITIL® Service Design) A set of tools, data, and information that is used to support information security management. The security management information system is part of the information security management system. See also service knowledge management system.
security policy	See information security policy.
threat	A threat is anything that might exploit a vulnerability. Any potential cause of an incident can be considered a threat. For example, a fire is a threat that could exploit the vulnerability of flammable floor coverings. This term is commonly used in information security management and IT service continuity management but also applies to other areas, such as problem and availability management.
vulnerability	A weakness that could be exploited by a threat—for example, an open firewall port, a password that is never changed, or a flammable carpet. A missing control is also considered to be a vulnerability.

Scope

THE INFORMATION SECURITY MANAGEMENT PROCESS should be the focal point for all IT security issues and must ensure that an information security policy is produced, maintained, and enforced that covers the use and misuse of all IT systems and services. Information security management needs to understand the total IT and business security environment, including the:

- Business security policy and plans
- Current business operation and its security requirements
- Future business plans and requirements
- Legislative and regulatory requirements
- Obligations and responsibilities with regard to security contained within SLAs
- The business and IT risks and their management

Understanding all of this will enable Information Security Management to ensure that all the current and future security aspects and risks of the business are cost-effectively managed.

Information Security Management ensures that the **confidentiality, integrity, and availability** of an organization's assets, information, data, and IT services is maintained. Information Security Management must consider the following four perspectives:

- Organizational—define security policies and staff awareness of these
- Procedural—defined procedures used to control security
- Physical—Controls used to protect any physical sites against security incidents
- Technical—Controls used to protect the IT infrastructure against security incidents

Information Security Management Policy

A CONSISTENT SET OF POLICIES and supporting documents should be developed to define the organization's approach to security, which is supported by all levels of management in the organization.

These policies should be made available to customers and users, and their compliance should be referred to in all SLRs, SLAs, contracts, and agreements. The policies should be authorized by top executive management within the business and

IT, and compliance to them should be endorsed on a regular basis. All security policies should be reviewed and, where necessary, revised on at least an annual basis.

The overall Information Security Policy should consist of a number of sub-components or sub-policies, covering:

- The use and misuse of IT assets
- Access control
- Password control
- E-mail
- Internet
- Anti-virus
- Information classification
- Document classification
- Remote access
- Supplier access
- Asset disposal

The Information Security Management System (ISMS)

THE ISMS CONTAINS THE STANDARDS, management procedures, and guidelines that support the Information Security Management policies. Using this in conjunction with an overall framework for managing security will help to ensure that the Four P's of People, Process, Products, and Partners are considered as to the requirements for security and control.

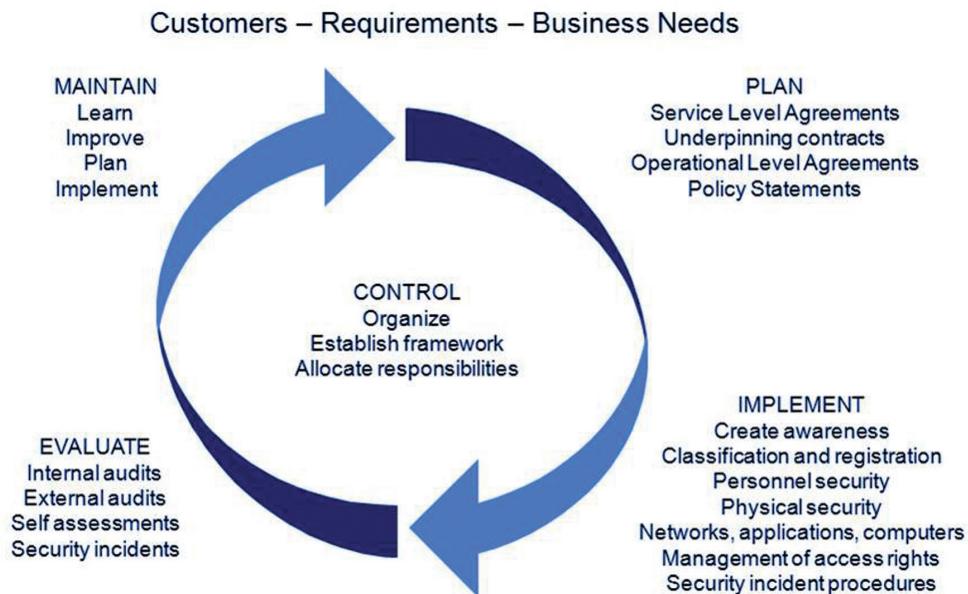


Figure 5.0—Framework for Managing IT Security

© Crown Copyright 2011 Reproduced under license from OGC

As a guide, standards such as ISO 27001 provide a formal standard by which to compare or certify their own ISMS, covering the five main elements of:

1. Plan

Planning is used to identify and recommend the appropriate security measures that will support the requirements and objectives of the organization. SLAs, OLAs, business and organizational plans and strategies, regulation and compliance requirements (such as Privacy Acts) as well as the legal, moral, and ethical responsibilities for information security will be considered in the development of these measures.

2. Implement

The objective of this element is to ensure that the appropriate measures, procedures, tools, and controls are in place to support the Information Security Policy.

3. Control

The objectives of the control element of the ISMS are to:

- Ensure the framework is developed to support Information Security Management
- Develop an organizational structure appropriate to support the Information Security Policy
- Allocate responsibilities
- Establish and control documentation

4. Evaluate

The evaluate element of the ISMS is focused on ensuring:

- Regular audits and reviews are performed
- Policy and process compliance is evaluated
- Information and audit reports are provided to management and external regulators, if required

5. Maintain

As part of Continual Service Improvement, the maintain element seeks to:

- Improve security agreements as documented in SLAs and OLAs
- Improve the implementation and use of security measures and controls

Activities

THE ACTIVITIES OF INFORMATION SECURITY Management are involved in multiple stages of the Service Lifecycle, including the:

- Development and maintenance of the Information Security Policy
- Communication, implementation, and enforcement of the security policies
- Assessment and classification of all information assets and documentation
- Implementation and continual review of appropriate security controls
- Monitoring and management of all security incidents
- Analysis, reporting, and reduction of the volumes and impact of security breaches and incidents
- Scheduling and execution of security reviews, audits, and penetration tests

Training and awareness is particularly vital and is often the weakness in an organization's control of security (particularly at the end-user stage). As part of the maintain element of the ISMS, consideration should be given to methods and techniques that can be improved so that the policies and standards can be more easily followed and implemented.

Inputs

INFORMATION SECURITY MANAGEMENT WILL NEED to obtain input from many areas, including:

- **Business information:** from the organization's business strategy, plans and financial plans, and information on its current and future requirements
- **Governance and security:** from corporate governance and business security policies and guidelines, security plans, risk assessment, and responses
- **IT information:** from the IT strategy and plans and current budgets
- **Service information:** from the SLM process with details of the services from the Service Portfolio and the Service Catalog, service level targets within SLAs and SLRs and possibly from the monitoring of SLAs, service reviews, and breaches of the SLAs

- **Risk assessment processes and reports:** from ISM, Availability Management and ITSCM
- **Details of all security events and breaches:** from all areas of IT and ITSM, especially Incident Management and Problem Management
- **Change information:** from the Change Management process with a change schedule and a need to assess all changes for their impact on all security policies, plans, and controls
- **CMS:** containing information on the relationships between the business, the services, supporting services, and the technology
- **Details of partner and supplier access:** from Supplier Management and Availability Management on external access to services and systems

Outputs

THE OUTPUTS PRODUCED BY THE Information Security Management process are used in all areas and should include:

- An overall information security management policy, together with a set of specific security policies
- A Security Management Information System (SMIS), containing all the information relating to Information Security Management
- Revised security risk assessment processes and reports
- A set of security controls, together with details of the operation and maintenance and their associated risks
- Security audits and audit reports
- Security test schedules and plans, including security penetration tests and other security tests and reports
- A set of security classifications and a set of classified information assets
- Reviews and reports of security breaches and major incidents
- Policies, processes, and procedures for managing partners and suppliers and their access to services and information

Service Design Summary

GOOD SERVICE DESIGN MEANS IT is possible to deliver quality, cost-effective services and to ensure that the business requirements are being met. It also delivers:

- Improved Quality of Service
- Improved Consistency of Service
- Improved Service Alignments
- Standards and Conventions to be followed
- More Effective Service Performance

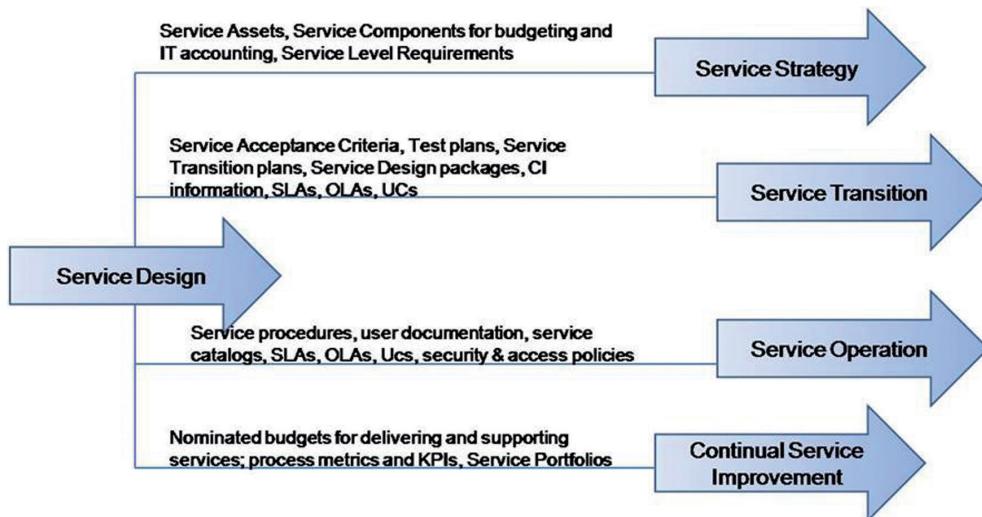


Figure 5.R—Example Service Design Outputs to Other Lifecycle Stages

Service Design Scenario

Design Coordination

- Comprehensive and consistent set of service designs and SDPs
- Revised measurement and metrics methods
- Service portfolio updated

Service Level Management Considerations

- SLR—detailed requirements that constitute the design criteria to be met, e.g., secure, clear uninterrupted voice, real time video, accessible for novice users, etc.
- SLA structure—decision made to develop multi-level structure (based on decision of service level package used, as well as offering greater security and accessibility to various departments/users)

Service Catalog Management Considerations

- Business Service Catalog—will describe HYPE service as business understands it, including levels of service
- Technical Services Catalog—will clearly list technical and supporting service information, e.g., ISP bandwidth, server requirements, etc.

Supplier Management Considerations

- Negotiate UCs with software vendor, ISP, WAN
- Monitor external supplier service—discussions with Availability Management, Service Desk, etc.

Capacity Management Considerations

- Application Sizing—assessing what minimum PC requirements needed to support new HYPE software, as well as type of webcam to best provide service, network bandwidth
- Modeling—how many users can videoconference before quality of service is affected, throughput/bandwidth targets, how may this service impact on other services?
- Demand Management—designing to ensure ability to limit bandwidth/video access during peak times for certain users/groups

Availability Management Considerations

- To ensure availability targets are met, regular maintenance of components is required, as well as ensuring through Supplier Management that ISP Underpinning Contract is met (serviceability requirements)

Information Security Management Considerations

- Confidentiality—user passwords design (e.g., HYPE service is not controlled locally; all information is stored on the vendor's server. If all users use the same password as their network login, resulting in a clear pattern, then it would be possible for security to be threatened if someone hacked into the vendor's server)
- Integrity—will logs of all conversations/messages/video kept be stored?
- Availability—having those logs available to those who require it, when they require it

ITSCM Considerations

- The business has decided that this is a BCP, so standby arrangements are negotiated with business (\$\$)
- Decided that the telephone line and/or email will be possible recovery measures until service is restored—included in ITSCM plan

The Service Design processes will ensure that HYPE meets the customer needs, can be developed and deployed by Service Transition, and then maintained and supported within Service Operation.

Service Design Review Questions

Question 1

Which ITIL® process analyzes threats and dependencies to IT services as part of the decision regarding countermeasures to be implemented?

- a) Availability Management
- b) IT Service Continuity Management
- c) Problem Management
- d) Service Asset and Configuration Management

Question 2

What is the name of the activity within the Capacity Management process whose purpose is to predict the future capacity requirements of new and changed services?

- a) Application Sizing
- b) Demand Management
- c) Modeling
- d) Tuning

Question 3

In which ITIL® process are negotiations held with customers about the availability and capacity levels to be provided?

- a) Availability Management
- b) Capacity Management
- c) Financial Management for IT Services
- d) Service Level Management

Question 4

Which of the following statements is false?

- a) It is impossible to maintain user and customer satisfaction during a disruption to service
- b) When reporting the availability provided for a service, the percentage (%) availability that is calculated takes into account the agreed service hours
- c) Availability of services could be improved by changes to the architecture, ITSM processes, or IT staffing levels
- d) Reports regarding availability should include more than just uptime, downtime, and frequency of failure and reflect the actual business impact of unavailability

Question 5

Which of the following activities is Service Level Management responsible for?

- a) Informing users of available services
- b) Identifying customer needs
- c) Overseeing service release schedule
- d) Keeping accurate records of all configuration items

Question 6

Which process reviews Operational Level Agreements (OLAs) on a regular basis?

- a) Supplier Management
- b) Service Level Management
- c) Service Portfolio Management
- d) Contract Management

Question 7

What is another term for Uptime?

- a) Mean Time Between Failures (MTBF)
- b) Mean Time to Restore Service (MTRS)
- c) Mean Time Between System Incidents (MTBSI)
- d) Relationship between MTBF and MTBSI

Question 8

Which of the following is an activity of IT Service Continuity Management?

- a) Advising end users of a system failure
- b) Documenting the recovery procedure for a critical system
- c) Reporting regarding availability
- d) Guaranteeing that the Configuration Items are constantly kept up - to - date

Question 9

Information security must consider the following four perspectives:

1. Organizational
2. Physical
3. Technical?
 - a) Process
 - b) Security
 - c) Procedural
 - d) Firewalls

Question 10

The 3 types of Service Level Agreements structures are:

- a) Customer-based, Service-based, Corporate-based
- b) Corporate-level, customer-level, service-level
- c) Service-based, customer-based, user-based
- d) Customer-based, service-based, multi-level

Chapter 6

Service Transition



Figure 6.A—Service Transition

The Service Transition lifecycle stage focuses on the vulnerable transition between the Design stage and the Operation stage of a service. It is particularly critical as functional and technical errors not found during this stage will result in significantly higher impact levels to the business and/or IT infrastructure and will usually cost much more to fix once the service is in operation.

Processes:

- Transition Planning and Support
- Knowledge Management
- Service Asset and Configuration Management
- Change Management
- Release and Deployment Management
- Service Validation and Testing
- Change Evaluation

THE ITIL® FOUNDATION CERTIFICATE IN ITSM syllabus and the corresponding exam requirements only cover five of these Service Transition processes, the other processes are covered in the Intermediate level of study. Therefore, this book and the corresponding eLearning program will cover the following Service Transition processes:

- Transition Planning and Support
- Knowledge Management
- Service Asset and Configuration Management
- Change Management
- Release and Deployment Management

Purpose

THE PRIMARY PURPOSE OF THE Service Transition stage of the Service Lifecycle is to ensure that any modifications or transitions to the live operational environment—affecting either new, modified, retiring, or retired services—meet the agreed expectations of the business, customers, and users. This means that all modifications to operational environments should be managed, planned, and coordinated through Service Transition processes and activities to facilitate a smooth transition to live operation. This will ensure that a new, modified, retiring, or retired service fulfils its operational expectation and has no or minimal adverse impact on customers, users, and the business.

Successful service transition does not happen until an organization recognizes the need for it and the benefits it will bring. Effective service transition is necessary because business operations and processes are in a constant state of transition. The quest for competitive advantage, best-of-breed innovation, agility, and self-preservation are eternal catalysts for changes that must ultimately be delivered.

Service Transition ensures that the requirements of Service Strategy encoded in Service Design are effectively realized through to the delivery of live services within the Service Operation stage of the Service Lifecycle. Service transition takes the outputs from Service Design, the preceding stage of the Lifecycle, and uses them to ensure that service solutions are smoothly migrated to live operation, fulfilling agreed customer and business requirements. The trigger for this transition activity is the production of a Service Design Package produced by the processes and activities of Service Design. Service Transition takes this new business requirement contained within the Service Design Package and, using the five aspects of design, creates services and their supporting practices that meet business demands for functionality, security, performance, reliability, and flexibility. The Service Design Package facilitates the build, test, and release and deployment activities of Service Transition and the operation, support, and improvement activities within the Service Operation and Continual Service Improvement stages of the Service Lifecycle.

The objectives of Service Transition are to:

- Plan and manage service changes efficiently and effectively
- Manage risks relating to new, changed, or retired services
- Successfully deploy service releases into supported environments

- Set correct expectations on the performance and use of new or changed services
- Ensure that service changes create the expected business value
- Provide good-quality knowledge and information about services and service assets

In order to achieve these objectives, there are many things that need to happen during the Service Transition Lifecycle stage. These include:

- Planning and managing the capacity and resources required to manage service transitions
- Implementing a rigorous framework for evaluating service capabilities and risk profiles before new or changed services are deployed
- Establishing and maintaining the integrity of service assets
- Providing efficient repeatable mechanisms for building, testing, and deploying services and releases
- Ensuring that services can be managed, operated, and supported in accordance with constraints specified during the Service Design stage of the Service Lifecycle

Value

SELECTING AND ADOPTING THE BEST practice as recommended in this publication will assist organizations in delivering significant benefits. It will help readers to set up Service Transition and the processes that support it and to make effective use of those processes to facilitate the effective transitioning of new, changed, or decommissioned services.

Adopting and implementing standard and consistent approaches for Service Transition will:

- Enable projects to estimate the cost, timing, resource requirement, and risks associated with the Service Transition stage more accurately
- Result in higher volumes of successful change
- Be easier for people to adopt and follow
- Enable Service Transition assets to be shared and re-used across projects and services

- Reduce delays from unexpected clashes and dependencies—for example, if multiple projects need to use the same test environment at the same time
- Reduce the effort spent on managing the Service Transition test and pilot environments
- Improve expectation setting for all stakeholders involved in Service Transition, including customers, users, suppliers, partners, and projects
- Increase confidence that the new or changed service can be delivered to specification without unexpectedly affecting other services or stakeholders
- Ensure that new or changed services will be maintainable and cost-effective
- Improve control of service assets and configurations

Service Transition Processes

Transition Planning and Support

EFFECTIVE TRANSITION PLANNING AND SUPPORT can significantly improve a service provider's ability to handle high volumes of change and releases across its customer base. An integrated approach to planning improves the alignment of the service transition plans with the customer, supplier, and business change project plans.

Purpose

THE PURPOSE OF THE TRANSITION planning and support process is to provide overall planning for service transitions and to coordinate the resources that they require.

The objectives of transition planning and support are to:

- Plan and coordinate the resources to ensure that the requirements of Service Strategy encoded in Service Design are effectively realized in Service Operation
- Coordinate activities across projects, suppliers, and service teams, where required
- Establish new or changed services into supported environments within the predicted cost, quality, and time estimates

- Establish new or modified management information systems and tools, technology and management architectures, service management processes, and measurement methods and metrics to meet requirements established during the Service Design Stage of the lifecycle
- Ensure that all parties adopt the common framework of standard re-usable processes and supporting systems in order to improve the effectiveness and efficiency of the integrated planning and coordination activities
- Provide clear and comprehensive plans that enable customer and business change projects to align their activities with the service transition plans
- Identify, manage, and control risks to minimize the chance of failure and disruption across transition activities and ensure that service transition issues, risks, and deviations are reported to the appropriate stakeholders and decision-makers
- Monitor and improve the performance of the Service Transition Lifecycle stage

Scope

THE SCOPE OF TRANSITION PLANNING and support includes:

- Maintaining policies, standards, and models for service transition activities and processes
- Guiding each major change or new service through all service transition processes
- Coordinating the efforts needed to enable multiple transitions to be managed at the same time
- Prioritizing conflicting requirements for service transition resources
- Planning the budget and resources needed to fulfill future requirements for service transition
- Reviewing and improving the performance of transition planning and support activities
- Ensuring that Service Transition is coordinated with program and project management, service design, and service development activities

Transition planning and support is not responsible for detailed planning of the build, test, and deployment of individual changes or releases; these activities are carried out as part of Change Management and Release and Deployment Management.

The transition planning and support process makes heavy use of the Service Knowledge Management System to provide access to the full range of information needed for short-, medium-, and long-range planning.

Transition planning and support needs access to information about new or changed services to create and manage plans. This information may be found in many structured and unstructured documents, such as guidelines, standards, models, and plans, as well as in documents created and maintained by other processes, such as Service Design Packages, contracts, Operational Level Agreements (OLAs), and process documentation. Timely access to up-to-date versions of these documents is essential so that transition plans can be created and managed. All of these documents should be stored in the Service Knowledge Management System (SKMS) and managed via Change Management and the CMS.

Inputs

THE INPUTS TO TRANSITION PLANNING and support are:

- Change proposal
- Authorized change
- Service Design Package, which includes:
 - Release package definition and design specification
 - Test plans
 - Deployment plans
 - Service acceptance criteria (SAC)

Outputs

THE OUTPUTS FROM TRANSITION PLANNING and support are:

- Transition strategy and budget
- Integrated set of service transition plans

Knowledge Management

THE QUALITY OF DECISION-MAKING WITHIN the Service Lifecycle depends on the ability and understanding of those parties involved, the understanding of the benefits and consequences of actions taken, and the analysis of any of the surrounding issues involved. All of this, in turn, depends on the availability of accurate and timely knowledge, information, and data provided in a way that can be easily accessed and interpreted by the appropriate parties.

That knowledge within the Service Transition domain might include:

- Identity of stakeholders
- Acceptable risk levels and performance expectations
- Available resource and timescales

The quality and relevance of the knowledge rests in turn on the accessibility, quality, and continued relevance of the underpinning data and information available to service staff.

Terminology

Term	Definition
data-to-information-to-knowledge-to-wisdom (DIKW)	(ITIL® Service Transition) A way of understanding the relationships between data, information, knowledge, and wisdom. DIKW shows how each of these builds on the others.
service knowledge management system (SKMS)	(ITIL® Service Transition) A set of tools and databases that is used to manage knowledge, information, and data. The service knowledge management system includes the configuration management system, as well as other databases and information systems. The service knowledge management system includes tools for collecting, storing, managing, updating, analyzing, and presenting all the knowledge, information, and data that an IT service provider will need to manage the full lifecycle of IT services.

Purpose

THE PURPOSE OF THE KNOWLEDGE Management process is to share perspectives, ideas, experience, and information to ensure that these are available in the right place at the right time to enable informed decisions and to improve efficiency by reducing the need to rediscover knowledge.

The objectives of Knowledge Management are to:

- Improve the quality of management decision-making by ensuring that reliable and secure knowledge, information, and data is available throughout the Service Lifecycle
- Enable the service provider to be more efficient and improve quality of service, increase satisfaction, and reduce the cost of service by reducing the need to rediscover knowledge
- Ensure that staff have a clear and common understanding of the value that their services provide to customers and the ways in which benefits are realized from the use of those services
- Maintain a Service Knowledge Management System (SKMS) that provides controlled access to knowledge, information, and data that is appropriate for each audience
- Gather, analyze, store, share, use, and maintain knowledge, information, and data throughout the service provider organization

Scope

WHILE KNOWLEDGE MANAGEMENT IS FOUND and primarily explained within the context of Service Transition, it is a process used by all elements of the Service Lifecycle to improve the decision-making that occurs.

What is not considered to be within the scope of Knowledge Management is the detailed configuration item information that is captured and maintained by Service Asset and Configuration Management (but is interfaced with the same tools and systems).

Benefits

WITH PARTICULAR FOCUS ON SERVICE Transition, knowledge is one of the important elements that need to be transitioned as part of the service changes and associated releases being managed. Examples where successful transition requires effective Knowledge Management include:

- User, service desk, support staff, and supplier understanding of the new or changed service, including knowledge of errors signed off before deployment, to facilitate their roles within that service
- Awareness of the use of the service and the discontinuation of previous versions
- Establishment of the acceptable risk and confidence levels associated with the transition

Outside of Service Transition, decision-making at the strategic, tactical, and operational levels all benefit from quality knowledge, information, and data being available. Some benefits include:

- Optimized service portfolios (with appropriate balance of investments, resources, services, and technology)
- Improved feedback loops between the design architects and the support staff for services
- Better real-time information and data for operational staff responding to user requests and incidents, as well as documented procedures for resolving known errors and requests

The Data Information Knowledge Wisdom (DIKW) Structure

KNOWLEDGE MANAGEMENT IS TYPICALLY DISPLAYED within the Data-to-Information-to-Knowledge-to-Wisdom (DIKW) structure. The use of these terms is set out below.

Data is a set of discrete facts. Most organizations capture significant amounts of data in highly structured databases, such as service management and service asset and configuration management tools/systems and databases.

The key knowledge management activities around data are the ability to:

- Capture accurate data
- Analyze, synthesize, and then transform the data into information
- Identify relevant data and concentrate resources on its capture
- Maintain integrity of the data
- Archive and purge data to ensure optimal balance between availability of data and use of resources

An example of data is the date and time at which an incident was logged.

Information comes from providing context to data. Information is typically stored in semi-structured content, such as documents, email, and multimedia. The key knowledge management activity around information is managing the content in a way that makes it easy to capture, query, find, re-use, and learn from experiences so that mistakes are not repeated and work is not duplicated.

An example of information is the average time to close priority 2 incidents. This information is created by combining data from the start time, end time, and priority of many incidents.

Knowledge is composed of the tacit experiences, ideas, insights, values, and judgments of individuals. People gain knowledge both from their own and from their peers' expertise, as well as from the analysis of information (and data). Through the synthesis of these elements, new knowledge is created.

Knowledge is dynamic and context-based. Knowledge puts information into an ease-of-use form, which can facilitate decision-making. In Service Transition, this knowledge is not solely based on the transition in progress but is gathered from experience of previous transitions, awareness of recent and anticipated changes, and other areas, which experienced staff will have been unconsciously collecting for some time.

An example of knowledge is that the average time to close priority 2 incidents has increased by about 10% since a new version of the service was released.

Wisdom makes use of knowledge to create value through correct and well-informed decisions. Wisdom involves having the application and contextual awareness to provide strong common-sense judgment.

An example of wisdom is recognizing that the increase in time to close priority 2 incidents is due to poor-quality documentation for the new version of the service.

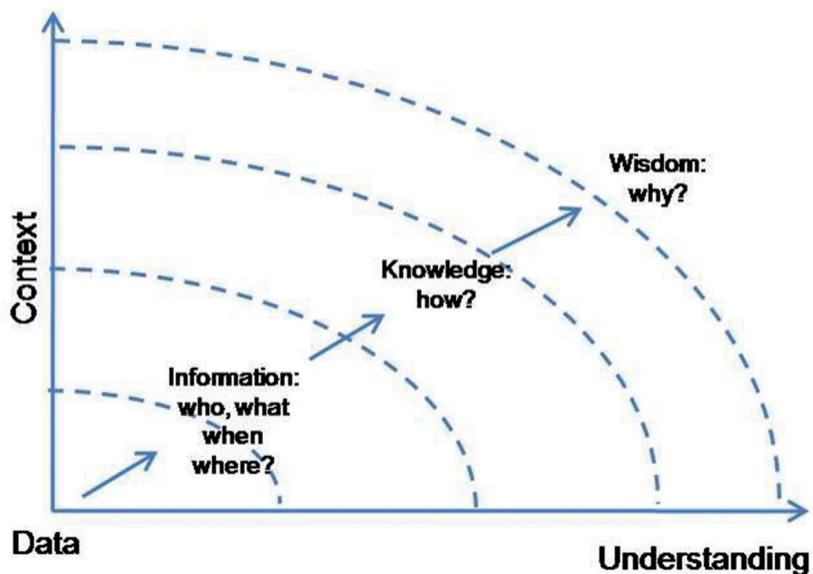


Figure 6.B—Moving from Data to Wisdom (DIKW Structure)

© Crown Copyright 2011 Reproduced under license from OGC

WE CAN USE TOOLS AND databases to capture data, information, and knowledge, but wisdom cannot be captured this way because wisdom is a concept relating to the ability to use knowledge to make correct judgments and decisions.

Service Knowledge Management System (SKMS)

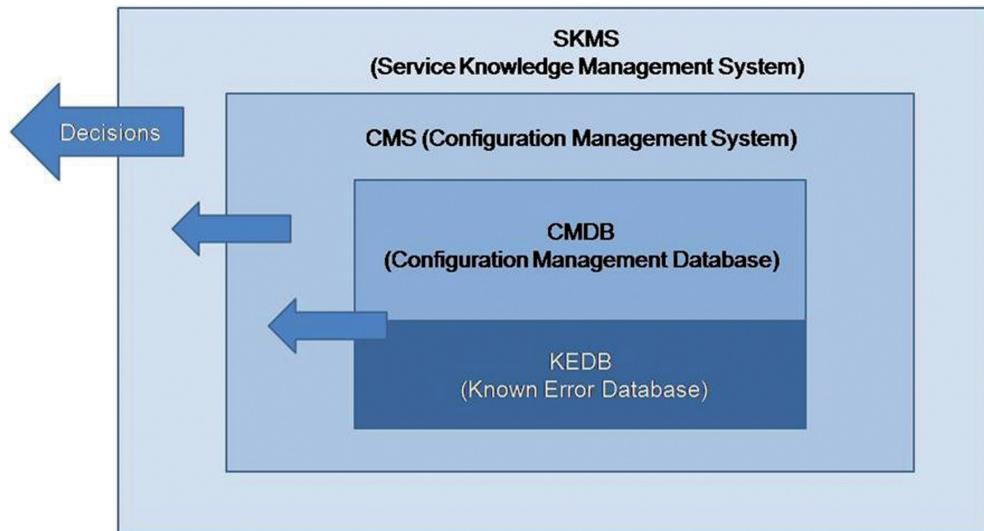


Figure 6.C—Components Making Up the Service Knowledge Management System

THE **SKMS** DESCRIBES THE COMPLETE set of tools and databases that are used to manage knowledge and information, including the Configuration Management System as well as other tools and databases. The SKMS stores, manages, updates, and presents all information that an IT service provider needs to manage the full lifecycle of its services. The main purpose of the SKMS is to provide quality information so that informed decisions can be made by the IT service provider.

Whereas the CMS focuses on providing information relating to the configuration of the IT infrastructure, the SKMS has a broader scope (as implied by the diagram), which includes anything pertaining to the needs of service management, including:

- Experience of staff
- Records of peripherals
- Supplier and partner requirements and abilities
- Typical and anticipated user skill levels

Service Asset and Configuration Management

Terminology

Term	Definition
attribute	(ITIL® Service Transition) A piece of information about a configuration item. Examples are name, location, version number, and cost. Attributes of CIs are recorded in a configuration management database (CMDB) and maintained as part of a configuration management system (CMS). See also relationship; configuration management system.
CI type	(ITIL® Service Transition) A category that is used to classify configuration items. The CI type identifies the required attributes and relationships for a configuration record. Common CI types include hardware, document, user, etc.
component	A general term that is used to mean one part of something more complex. For example, a computer system may be a component of an IT service; an application may be a component of a release unit. Components that need to be managed should be configuration items.
configuration	(ITIL® Service Transition) A generic term used to describe a group of configuration items that work together to deliver an IT service or a recognizable part of an IT service. Configuration is also used to describe the parameter settings for one or more configuration items.
configuration baseline	(ITIL® Service Transition) The baseline of a configuration that has been formally agreed and is managed through the change management process. A configuration baseline is used as a basis for future builds, releases, and changes.
configuration item (CI)	(ITIL® Service Transition) Any component or other service asset that needs to be managed in order to deliver an IT service. Information about each configuration item is recorded in a configuration record within the configuration management system and is maintained throughout its lifecycle by service asset and configuration management. Configuration items are under the control of change management. They typically include IT services, hardware, software, buildings, people, and formal documentation, such as process documentation and service level agreements.

Term	Definition
configuration management database (CMDB)	(ITIL® Service Transition) A database used to store configuration records throughout their lifecycle. The configuration management system maintains one or more configuration management databases, and each database stores attributes of configuration items and relationships with other configuration items.
configuration management system (CMS)	(ITIL® Service Transition) A set of tools, data, and information that is used to support service asset and configuration management. The CMS is part of an overall service knowledge management system and includes tools for collecting, storing, managing, updating, analyzing, and presenting data about all configuration items and their relationships. The CMS may also include information about incidents, problems, known errors, changes, and releases. The CMS is maintained by service asset and configuration management and is used by all IT service management processes.
	See also configuration management database.
configuration record	(ITIL® Service Transition) A record containing the details of a configuration item. Each configuration record documents the lifecycle of a single configuration item. Configuration records are stored in a configuration management database and maintained as part of a configuration management system.
relationship	A connection or interaction between two people or things. In business relationship management, it is the interaction between the IT service provider and the business. In service asset and configuration management, it is a link between two configuration items that identifies a dependency or connection between them. For example, applications may be linked to the servers they run on, and IT services have many links to all the configuration items that contribute to that IT service.
service asset	Any resource or capability of a service provider.
	See also asset.
status accounting	(ITIL® Service Transition) The activity responsible for recording and reporting the lifecycle of each configuration item.
verification and audit	(ITIL® Service Transition) The activities responsible for ensuring that information in the configuration management system is accurate and that all configuration items have been identified and recorded. Verification includes routine checks that are part of other processes—for example, verifying the serial number of a desktop PC when a user logs an incident. Audit is a periodic, formal check.

Purpose

THE PURPOSE OF THE SERVICE Asset and Configuration Management (SACM) process is to ensure that the assets required to deliver services are properly controlled and that accurate and reliable information about those assets is available when and where it is needed. This information includes details of how the assets have been configured and the relationships between assets.

The objectives of SACM are to:

- Ensure that assets under the control of the IT organization are identified, controlled, and properly cared for throughout their lifecycle
- Identify, control, record, report, audit, and verify services and other configuration items (CIs), including versions, baselines, constituent components, their attributes, and relationships
- Account for, manage, and protect the integrity of CIs through the Service Lifecycle by working with Change Management to ensure that only authorized components are used and only authorized changes are made
- Ensure the integrity of CIs and configurations required to control the services by establishing and maintaining an accurate and complete Configuration Management System (CMS)
- Maintain accurate configuration information on the historical, planned, and current state of services and other CIs
- Support efficient and effective service management processes by providing accurate configuration information to enable people to make decisions at the right time—for example, to authorize changes and releases or to resolve incidents and problems

Scope

SERVICE ASSETS THAT NEED TO be managed in order to deliver services are known as configuration items (CIs). Other service assets may be required to deliver the service, but, if they cannot be individually managed, then they are not configuration items. Every CI is a service asset, but many service assets are not CIs. For example, a server will be both a CI and an asset; the knowledge used by an experienced service desk person to manage incidents is an important asset but is not a CI. Also, information that is stored on the server but is not under the control of Change Management may be a very valuable asset, but it is not a configuration item. It is important to note that many virtual assets, such as virtual servers or networks, may be CIs and require the same management control as physical assets.

The scope of SACM includes management of the complete lifecycle of every CI.

Service Asset and Configuration Management ensures that CIs are identified, baselined, and maintained and that changes to them are controlled. It also ensures that releases into controlled environments and operational use are done on the basis of formal authorization. It provides a configuration model of the services and service assets by recording the relationships between configuration items. SACM may cover non-IT assets, work products used to develop the services, and CIs required to support the service that would not be classified as assets by other parts of the business.

The scope includes interfaces to internal and external service providers where there are assets and configuration items that need to be controlled, e.g., shared assets.

Most organizations have a process that tracks and reports the value and ownership of fixed assets throughout their lifecycle. This process is usually called *Fixed Asset Management* or *Financial Asset Management*. Fixed Asset Management maintains an asset register, which records financial information about all of the organization's fixed assets. Fixed Asset Management is not usually under the control of the same business unit as the IT services, but the SACM process must provide proper care for the fixed assets under the control of IT and there must be well-defined interfaces between SACM and Fixed Asset Management. Data from the asset register may be integrated with the Configuration Management System to provide a more complete view of the CIs.

The Configuration Management Database (CMDB)

THE CMDB IS A SET of one or more connected databases and information sources that provide a logical model of the IT infrastructure. It captures Configuration Items (CIs) and the relationships that exist between them. Figure 6.D demonstrates the elements of a CMDB.

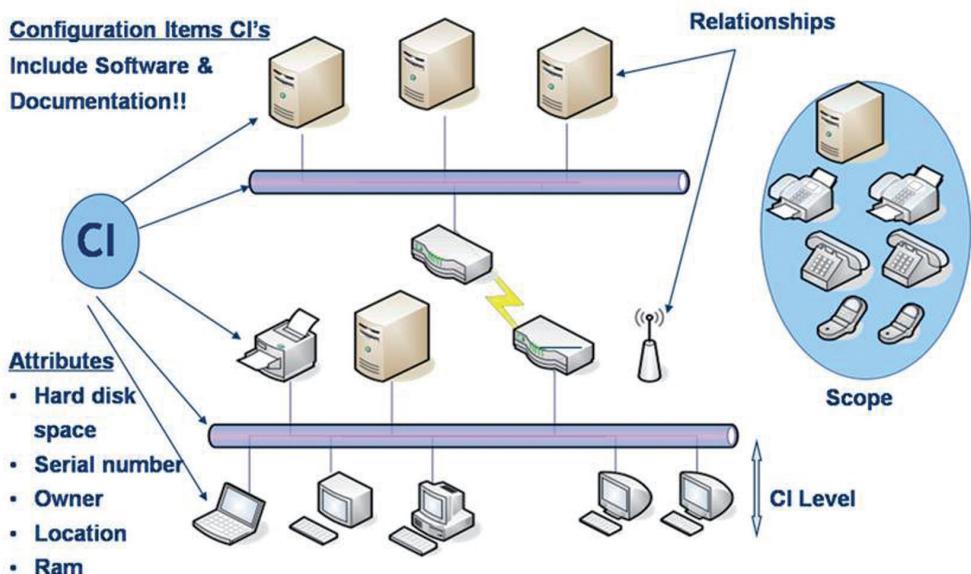


Figure 6.D—The Configuration Management Database (CMDB)

AS THE ABOVE FIGURE SHOWS, it is important to determine the level to which the CMDB will record information about the IT infrastructure and to decide what is not covered within the scope of the CMDB. Components out of scope are those typically not under the control of Change Management (e.g., telecommunication equipment). The CMS is also used for a wide range of purposes, including business processes where information is required for financial, compliance, HR, or other reasons.

At the data level, the CMS may be formed by a combination of physical Configuration Management Databases (CMDBs), as well as other sources they feed and interface information together. Wherever possible, the CMS should provide access to information for other inventories rather than duplicating the data captured. Automation is a factor for success for larger CMS deployments, with discovery,

inventory, audit, network management, and other tools being used with interfaces to the CMS.

Activities



Figure 6.E—Service Asset and Configuration Management Activities

NOTICE HOW MANAGEMENT AND PLANNING are the central activities. Good, sound Service Asset and Configuration Management requires thorough planning for the operation of the process to work.

Planning:

- Defining the strategy, policy, scope, objectives, processes, and procedures for Service Asset and Configuration Management
- Roles and responsibilities of involved staff and stakeholders
- Location of storage areas and libraries used to hold hardware, software, and documentation
- CMDB design
- CI naming conventions
- Housekeeping, including license management and archiving of CIs

Identification: includes the selection, identification, labeling, and registration of CIs. It is the activity that determines what CIs will be recorded, what their attributes are, and what relationships exist with other CIs. Identification can take place for:

- Hardware and software—including OS
- Business systems—custom built
- Packages—off the shelf
- Physical databases
- Feeds between databases and links
- Configuration baselines
- Software releases
- Documentation

Control: where the CMDB is utilized to store or modify configuration data. Effective control ensures that only authorized and identifiable CIs are recorded from receipt to disposal in order to protect the integrity of the CMDB. Control occurs anytime the CMDB is altered, including:

- Registration of all new CIs and versions
- Updating of CI records and license control
- Updates in connection with RFCs and Change Management
- Updating the CMDB after periodic checking of physical items

Status Accounting: the reporting of all current and historical data concerned with each CI throughout its lifecycle. Provides information on:

- Configuration baselines
- Latest software item versions
- The person responsible for status change
- CI change/incident/problem history

Verification and Audit: reviews and audits verify the existence of CIs, checking that they are correctly recorded in the CMDB and that there is conformity between the documented baselines and the actual environment to which they refer. Configuration audits should occur at the following times:

- Before and after major changes to the IT infrastructure
- Following recovery from disaster
- In response to the detection of an unauthorized CI
- At regular intervals

Benefits

THE MAJORITY OF BENEFITS ENABLED by effective Service Asset and Configuration Management can be seen in improvements of other Service Management processes. By having quality asset and configuration data available, the benefits to other processes include:

- Better forecasting and planning of changes
- Changes and releases to be assessed, planned, and delivered successfully
- Incidents and problems to be resolved within the service level targets
- Changes to be traceable from requirements
- Enhanced ability to identify the costs for a service

Benefits that may be seen to be provided primarily by the process alone include:

- Better adherence to standards
- Greater compliance to legal and regulatory obligations
- Optimum software licensing by ensuring correlation between licenses needed against the number of purchases
- The data about CIs and methods of controlling CIs is consolidated—reduces auditing effort
- Opens opportunities for consolidation in CIs to support services

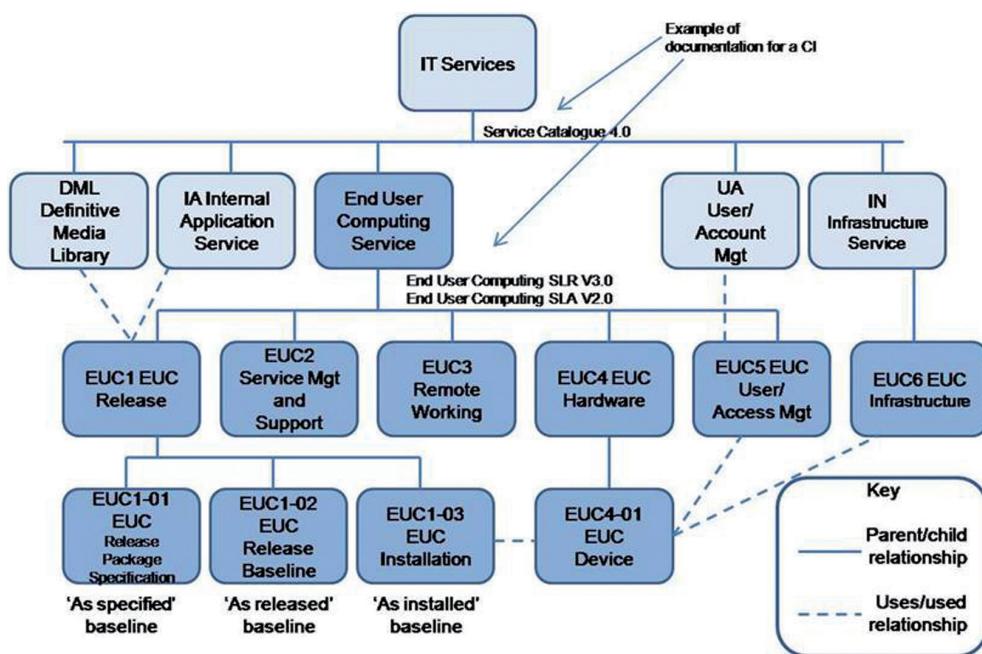


Figure 6.F—Example Configuration Breakdown for an IT Service

© Crown Copyright 2011 Reproduced under license from OGC

Inputs

- Inputs to Service Asset and Configuration Management include:
- Designs, plans, and configurations from Service Design Packages
- Requests for change and work orders from Change Management
- Actual configuration information collected by tools and audits
- Information in the organization's fixed asset register

Outputs

OUTPUTS FROM SERVICE ASSET AND Configuration Management include:

- New and updated configuration records
- Updated asset information for use in updating the fixed asset register
- Information about attributes and relationships of configuration items for use by all other service management processes. This information should be presented in appropriate views for each audience
- Configuration snapshots and baselines

- Status reports and other consolidated configuration information
- Audit reports

Change Management

THE ABILITY TO CONTROL AND manage changes to defined IT services and their supporting elements is viewed as a fundamental part of quality service management. When reviewing the typical strategic objectives of an IT service provider, most of these are underpinned by the requirement of effective change control. These include strategies focusing on time-to-market, increased market share or high availability, and security platforms, all of which require a controlled process by which to assess, control, and manage changes with varying levels of rigor.

Changes arise for a number of reasons:

- From requests of the business or customers, seeking to improve services, reduce costs, or increase ease and effectiveness of delivery and support
- From internal IT groups looking to proactively improve services or to resolve errors and correct service disruption

The process of Change Management typically exists in order to:

- Optimize risk exposure (defined from both business and IT perspectives)
- Minimize the severity of any impact or disruption
- Deliver successful changes at the first attempt

To deliver these benefits while being careful not to cause excessive delays or bottlenecks as part of a coordinated approach to Service Transition, it is important to consider the diverse types of changes that will be assessed and how a balance can be maintained in regards to the varying needs and potential impacts of changes. In light of this, it is important to interpret the following Change Management guidance with the understanding that is intended to be scaled to suit the organization and the size, complexity, and risk of changes being assessed.

Terminology

Term	Definition
change	(ITIL® Service Transition) The addition, modification, or removal of anything that could have an effect on IT services. The scope should include changes to all architectures, processes, tools, metrics, and documentation, as well as changes to IT services and other configuration items.
change advisory board (CAB)	(ITIL® Service Transition) A group of people that support the assessment, prioritization, authorization, and scheduling of changes. A change advisory board is usually made up of representatives from all areas within the IT service provider, the business, and third parties, such as suppliers.
change model	(ITIL® Service Transition) A repeatable way of dealing with a particular category of change. A change model defines specific agreed steps that will be followed for a change of this category. Change models may be very complex with many steps that require authorization (e.g., major software release) or may be very simple with no requirement for authorization (e.g., password reset).
	See also change advisory board; standard change.
change proposal	(ITIL® Service Strategy) (ITIL® Service Transition) A document that includes a high level description of a potential service introduction or significant change, along with a corresponding business case and an expected implementation schedule. Change proposals are normally created by the service portfolio management process and are passed to change management for authorization. Change management will review the potential impact on other services, on shared resources, and on the overall change schedule. Once the change proposal has been authorized, service portfolio management will charter the service.
change record	(ITIL® Service Transition) A record containing the details of a change. Each change record documents the lifecycle of a single change. A change record is created for every request for change that is received, even those that are subsequently rejected. Change records should reference the configuration items that are affected by the change. Change records may be stored in the configuration management system or elsewhere in the service knowledge management system.
change request	See request for change.

Term	Definition
change schedule	(ITIL® Service Transition) A document that lists all authorized changes and their planned implementation dates, as well as the estimated dates of longer-term changes. A change schedule is sometimes called a forward schedule of change, even though it also contains information about changes that have already been implemented.
emergency change	(ITIL® Service Transition) A change that must be introduced as soon as possible—for example, to resolve a major incident or implement a security patch. The change management process will normally have a specific procedure for handling emergency changes.
	See also emergency change advisory board.
emergency change advisory board (ECAB)	(ITIL® Service Transition) A subgroup of the change advisory board that makes decisions about emergency changes. Membership may be decided at the time a meeting is called and depends on the nature of the emergency change.
normal change	(ITIL® Service Transition) A change that is not an emergency change or a standard change. Normal changes follow the defined steps of the change management process.
remediation	(ITIL® Service Transition) Actions taken to recover after a failed change or release. Remediation may include back-out, invocation of service continuity plans, or other actions designed to enable the business process to continue.
request for change (RFC)	(ITIL® Service Transition) A formal proposal for a change to be made. It includes details of the proposed change and may be recorded on paper or electronically. The term is often misused to mean a change record or the change itself.
standard change	(ITIL® Service Transition) A pre-authorized change that is low risk, relatively common, and follows a procedure or work instruction—for example, a password reset or provision of standard equipment to a new employee. Requests for change are not required to implement a standard change, and they are logged and tracked using a different mechanism, such as a service request.
	See also change model.

Purpose

THE PURPOSE OF THE CHANGE Management process is to control the lifecycle of all changes, enabling beneficial changes to be made with minimum disruption to IT services.

The objectives of Change Management are to:

- Respond to the customer's changing business requirements, while maximizing value and reducing incidents, disruption, and re-work
- Respond to the business and IT requests for change that will align the services with the business needs
- Ensure that changes are recorded and evaluated and that authorized changes are prioritized, planned, tested, implemented, documented, and reviewed in a controlled manner
- Ensure that all changes to configuration items are recorded in the configuration management system
- Optimize overall business risk—it is often correct to minimize business risk, but sometimes it is appropriate to knowingly accept a risk because of the potential benefit.



Figure 6.G—Change Management

CHANGE MANAGEMENT ACTS AS the greatest contributor to the CMDB, as changes to the CMDB must be assessed and authorized by Change Management first.

To work effectively, Change Management needs to remain impartial to the needs of any one particular IT group or customer in order to make effective decisions that best support the overall organizational objectives.

Scope

THE TERM ‘**CHANGE**’ HAS MANY meanings; however, the best definition of a service change is:

“Any alteration in the state of a Configuration Item (CI). This includes the addition, modification, or removal of approved, supported, or baselined hardware, network, software, application, environment, system, desktop build, or associated documentation.”

It is important that every organization defines those changes that lie outside the scope of their service change process (such as operational or business process and policy changes).

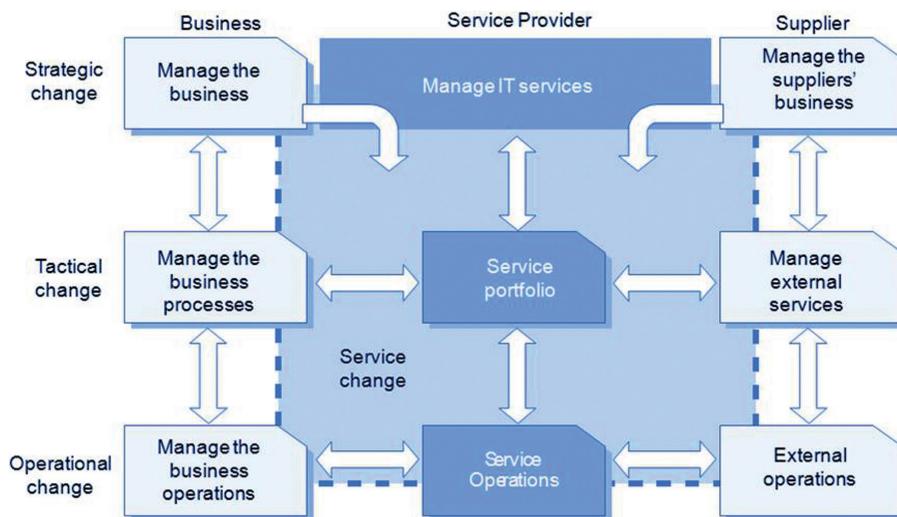


Figure 6.H—Scope of Change Management for IT Services

© Crown Copyright 2011 Reproduced under license from OGC

THIS FIGURE DEMONSTRATES THE TYPICAL scope of the Change Management process for an IT service provider and how it interfaces with the business and suppliers at strategic, tactical, and operational levels. As discussed in Service Strategy, Service Portfolios provide the clear definition of all planned, current, and retired services.

"Remember: Not every change is an improvement, but every improvement is a change!"

Change Models

THE DEFINITION OF DIFFERENT PROCESS models will allow an organization to maintain a balance between providing an appropriate level of control for changes without causing bottlenecks or restricting business growth. Change Models define how various categories of changes are assessed and authorized with different mechanisms and activities used to process and deliver changes based on the change type. The defined Change Models should also include:

- What steps should be taken to manage the change
- Roles and responsibilities
- Timescales and thresholds for actions
- Escalation procedures

Change Models defined within ITIL® include the following:

NORMAL Change: A change that follows all of the steps of the change process. It is assessed by either a Change Manager or Change Advisory Board. Normal changes will often be further defined by the relative impact and complexity, which will escalate the change for assessment to the most appropriate person or group.

STANDARD Change: A *pre-approved* change that is low risk, relatively common, and follows a procedure or work instruction. E.g., password reset or provision of standard equipment to a new employee. RFCs are not required to implement a standard change, and they are logged and tracked using a different mechanism, such as a **service request**. While standard changes are effectively pre-approved by Change Management, they may still require forms of authorization, such as by other groups like Human Resources (HR) or financial departments.

The main elements of a standard change are that:

- Authority is effectively given in advance
- The tasks are well known, documented, and proven
- There is a defined trigger to initiate the Request For Change (RFC)
- Budgetary approval is typically defined or controlled by the requester
- The risk is usually low and always well understood

Over time and as the IT organization matures, the list of standard changes should increase in order to maintain optimum levels of efficiency and effectiveness.

EMERGENCY Change: A change that must be introduced as soon as possible, e.g., to resolve a major incident or implement a security patch.

The Change Management process will normally have a specific procedure for handling emergency changes quickly without sacrificing normal management controls. Organizations should be careful to ensure that the number of emergency changes be kept to a minimum because they are typically more disruptive and prone to failure.

To enable this to occur, methods of assessment and documentation are typically modified with some documentation occurring after the change has occurred.

Activities

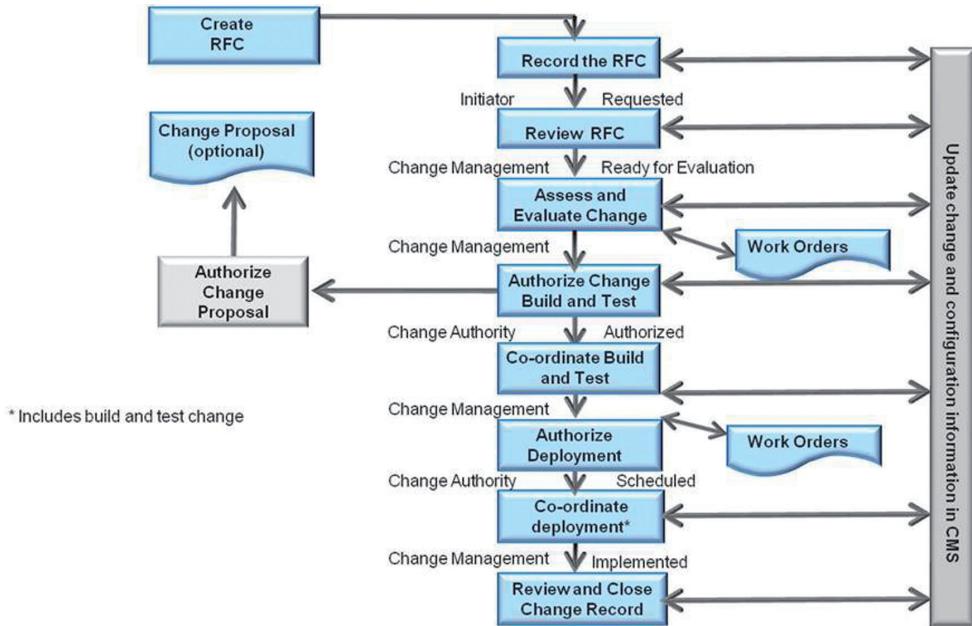


Figure 6.1—The Activities of Change Management

© Crown Copyright 2011 Reproduced under license from OGC

Where can RFCs be initiated?

Anywhere (Other ITIL® processes, customers, end-users etc.)

Who does the actual build/test/implement?

- Technical areas
- Project teams
- Release and Deployment Management

Important Steps:

1. The RFC is logged
2. An initial review is performed (to filter RFCs)
3. The RFCs are assessed—may require involvement of CAB or ECAB
4. Authorization of change build and test by the Change Manager
5. Coordination of the build and test, e.g., work orders are issued for the build of the change (carried out by other groups)

6. Change Management authorizes deployment
7. Change Management coordinates the deployment (with multiple checkpoints)
8. The change is reviewed (Post Implementation Review)
9. The change is closed

Change Proposals

MAJOR CHANGES THAT INVOLVE SIGNIFICANT cost, risk, or organizational impact will usually be initiated through the Service Portfolio Management process. Before the new or changed service is chartered, it is important that the change is reviewed for its potential impact on other services, on shared resources, and on the change schedule.

Change proposals are submitted to Change Management before chartering new or changed services in order to ensure that potential conflicts for resources or other issues are identified. Authorization of the change proposal does not authorize implementation of the change but simply allows the service to be chartered so that service design activity can commence.

A change proposal is used to communicate a high-level description of the change. This change proposal is normally created by the Service Portfolio Management process and is passed to Change Management for authorization. In some organizations, change proposals may be created by a program management office or by individual projects. The change proposal should include:

- A high-level description of the new, changed, or retired service, including business outcomes to be supported and utility and warranty to be provided
- A full business case including risks, issues, and alternatives, as well as budget and financial expectations
- An outline schedule for design and implementation of the change

Change Management reviews the change proposal and the current change schedule, identifies any potential conflicts or issues, and responds to the change proposal by either authorizing it or documenting the issues that need to be resolved.

When the change proposal is authorized, the change schedule is updated to include outline implementation dates for the proposed change.

After the new or changed service is chartered, RFCs will be used in the normal way to request authorization for specific changes. These RFCs will be associated with the change proposal so that Change Management has a view of the overall strategic intent and can prioritize and review these RFCs appropriately.

Remediation planning

NO CHANGE SHOULD BE AUTHORIZED without having explicitly addressed the question of what to do if it is not successful. Ideally, there will be a back-out plan, which will restore the organization to its initial state, often through the reloading of a baselined set of Cls, especially software and data. However, not all changes are reversible, in which case an alternative approach to remediation is required.

This remediation may require a revisiting of the change itself in the event of failure or may be so severe that it requires invoking the organization's business continuity plan. Only by considering what remediation options are available before instigating a change and by establishing that the remediation is viable (e.g., it is successful when tested) can the risk of the proposed change be determined and appropriate decisions taken.

Change implementation plans should include milestones and other triggers for implementation of remediation in order to ensure that there is sufficient time in the agreed change window for back-out or other remediation when necessary.

Assessing and Evaluating Changes

TO ENSURE THAT THE CHANGE Management process does not become a bottleneck, it is important to define what Change Models will be used to ensure effective and efficient control and implementation of RFCs.

Level	Change Authority	Potential Impact/Risk
1	Business Executive Board	High cost/risk change—executive decision
2	The IT Management (Steering) Board	Change impacts multiple services/organizational divisions
3	Change Advisory Board (CAB) or Emergency CAB (ECAB)	Change impacts only local/service group
4	Change Manager	Change to a specific component of an IT Service
5	Local Authorization	Standard change

Authorization of Changes

WHILE THE RESPONSIBILITY FOR AUTHORIZATION for changes lies with the Change Manager, they in turn will ensure they have the approval of three main areas:

- Financial Approval—what is it going to cost? And what is the cost of not doing it?
- Business Approval—what are the consequences to the business? And what are the consequences of not doing it?
- Technology Approval—what are the consequences to the infrastructure? And what are the consequences of not doing it?

Key Points:

- Change Management should consider the implications of performing the change as well as the impacts of NOT implementing the change
- Importance of empowering Change Manager as their primary role is to protect the integrity of the IT infrastructure

Relationship with Project Management:

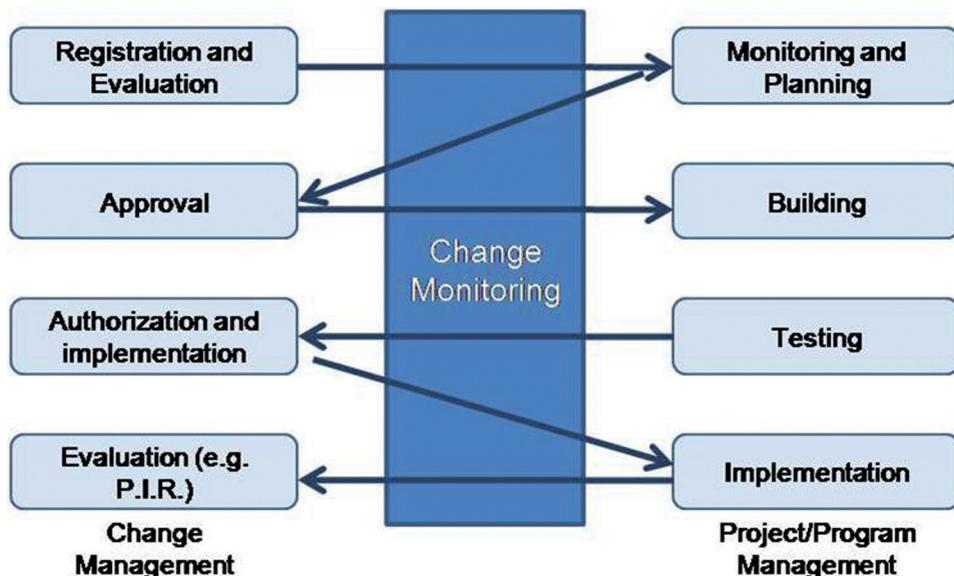


Figure 6.J—Relationship with Project Management

© Crown Copyright 2011 Reproduced under license from OGC

How does Change Management work with Project Management?

- Change Management authorizes, controls, and coordinates changes but does not plan, build, test, or implement changes
- Change Management is concerned with Remediation Planning to ensure that each RFC has a fallback/rollback plan

Roles and Responsibilities

- **Change Manager**
 - Administration of all RFCs
 - Prepare RFCs for CAB meetings, communicate change schedule for Service Desk
 - Authorize (or reject) changes
- **Change Advisory Board (CAB)**
- Advises Change Manager on authorization issues for RFCs with significant or major impact

- Typical representatives for a CAB under normal conditions are:
 - The Change Manager (chairs the CAB)
 - Customer representatives
 - User management
 - Application Developers/Supporters
 - Technical Experts and Consultants
 - Other Services Staff
 - Vendors and Suppliers

Rather than having a static list of members, the CAB should include both static and dynamic members who will attend based on the needs for the changes being discussed.

Inputs

CHANGES MAY BE SUBMITTED AS an RFC, often with an associated change proposal that provides inputs from the Service Strategy stage of the Service Lifecycle. The inputs include:

- Policy and strategy for change and release
- Request for change
- Change proposal
- Plans—change, transition, release, test, evaluation, and remediation
- Current change schedule and PSO
- Evaluation reports and interim evaluation reports
- Current assets or configuration items, e.g., baseline, service package, release package
- As-planned configuration baseline
- Test results, test report, and evaluation report

Outputs

Outputs from the process will be:

- Rejected and cancelled RFCs
- Authorized changes
- Authorized change proposals
- Change to the services, service, or infrastructure resulting from authorized changes

- New, changed, or disposed configuration items, e.g., baseline, service package, release package
- Revised change schedule
- Revised PSO
- Authorized change plans
- Change decisions and actions
- Change documents and records
- Change management reports

Release and Deployment Management

Often forgotten or ignored in many IT Service Management implementations or initiatives, Release and Deployment can be mistakenly seen as the poor cousin of Change Management—of less importance and priority to both the business and IT organizations.

Much of the confusion and misunderstanding is perpetuated by the idea that Release and Deployment only focuses on the actual distribution of changes to the live environment. While timely and accurate distribution is indeed a goal of the process, the actual scope includes all of the activities, systems, and functions required to build, test, and deploy a release into production and enable effective handover to service operations.

In conjunction with the use of Change Management, Release and Deployment will enhance an organization's capabilities to develop, compile, reuse, distribute, and rollback releases in accordance with defined policies that improve efficiency and reduce business disruption.

Terminology

Term	Definition
build	(ITIL® Service Transition) The activity of assembling a number of configuration items to create part of an IT service. The term is also used to refer to a release that is authorized for distribution—for example, server build or laptop build.
	See also configuration baseline.
definitive media library (DML)	(ITIL® Service Transition) One or more locations in which the definitive and authorized versions of all software configuration items are securely stored. The definitive media library may also contain associated configuration items, such as licenses and documentation. It is a single logical storage area, even if there are multiple locations. The definitive media library is controlled by service asset and configuration management and is recorded in the configuration management system.
deployment	(ITIL® Service Transition) The activity responsible for movement of new or changed hardware, software, documentation, process, etc. to the live environment. Deployment is part of the release and deployment management process.
release	(ITIL® Service Transition) One or more changes to an IT service that are built, tested, and deployed together. A single release may include changes to hardware, software, documentation, processes, and other components.
release package	(ITIL® Service Transition) A set of configuration items that will be built, tested, and deployed together as a single release. Each release package will usually include one or more release units.
release record	(ITIL® Service Transition) A record that defines the content of a release. A release record has relationships with all configuration items that are affected by the release. Release records may be in the configuration management system or elsewhere in the service knowledge management system.
release unit	(ITIL® Service Transition) Components of an IT service that are normally released together. A release unit typically includes sufficient components to perform a useful function. For example, one release unit could be a desktop PC, including hardware, software, licenses, documentation, etc. A different release unit may be the complete payroll application, including IT operations procedures and user training.
release window	See change window.
test	(ITIL® Service Transition) An activity that verifies that a configuration item, IT service, process, etc. meets its specification or agreed requirements.

Purpose

THE PURPOSE OF THE RELEASE and Deployment Management process is to plan, schedule, and control the build, test, and deployment of releases and to deliver new functionality required by the business while protecting the integrity of existing services.

The objectives of Release and Deployment Management are to:

- Define and agree Release and Deployment Management plans with customers and stakeholders
- Create and test release packages that consist of related configuration items that are compatible with each other
- Ensure that the integrity of a release package and its constituent components is maintained throughout the transition activities and that all release packages are stored in a DML and recorded accurately in the CMS
- Deploy release packages from the DML to the live environment following an agreed plan and schedule
- Ensure that all release packages can be tracked, installed, tested, verified, and/or uninstalled or backed out if appropriate
- Ensure that organization and stakeholder change is managed during release and deployment activities (see Chapter 5)
- Ensure that a new or changed service and its enabling systems, technology, and organization are capable of delivering the agreed utility and warranty
- Record and manage deviations, risks, and issues related to the new or changed service and take necessary corrective action
- Ensure that there is knowledge transfer to enable the customers and users to optimize their use of the service to support their business activities
- Ensure that skills and knowledge are transferred to service operation functions to enable them to effectively and efficiently deliver, support, and maintain the service according to required warranties and service levels.

Scope

THE SCOPE OF RELEASE AND Deployment Management includes the processes, systems, and functions to package, build, test, and deploy a release into live use, establish the service specified in the Service Design Package, and formally hand the service over to the service operation functions. The scope includes all configuration items required to implement a release, for example:

- Physical assets, such as a server or network
- Virtual assets, such as a virtual server or virtual storage
- Applications and software
- Training for users and IT staff
- Services, including all related contracts and agreements

Although Release and Deployment Management is responsible for ensuring that appropriate testing takes place, the actual testing is carried out as part of the service validation and testing process.

Release and deployment management is not responsible for authoring changes and requires authorization from Change Management at various stages in the lifecycle of a release.

Effective Release and Deployment Management enables the service provider to add value to the business by:

- Delivering change faster and at optimum cost and minimized risk
- Assuring that customers and users can use the new or changed service in a way that supports the business goals
- Improving consistency in implementation approach across the business change, service teams, suppliers, and customers
- Contributing to meeting auditable requirements for traceability through service transition

Well-planned and implemented Release and Deployment Management will make a significant difference to an organization's service costs. A poorly designed release or deployment will, at best, force IT personnel to spend significant amounts of time troubleshooting problems and managing complexity. At worst, it can cripple the environment and degrade live services.

Release and Deployment Management also works closely with Change Management and the Service Desk to inform users of scheduled changes/deployments. Tools used to do this can include:

- E-mail notification
- SMS notification
- Verbal communication

Release Policy

A **RELEASE POLICY** IS THE formal documentation of the overarching strategy for releases and was derived from the Service Design stage of the Service Lifecycle. It is the governing policy document for the process and must accommodate the majority of releases being implemented. Typical contents of a Release Policy include:

- Level of infrastructure to be controlled by releases
- Preferred structure and schedules for release packages
- Definition of major and minor releases, emergency fixes
- Expected deliverables for each type of release
- Policy on the production and execution of back out plans
- How and where releases should be documented
- Blackout windows for releases based on business or IT requirements
- Roles and responsibilities defined for the Release and Deployment process
- Supplier contacts and escalation points

Four phases of Release and Deployment Management

THERE ARE FOUR PHASES TO Release and Deployment Management (see Figure 6.K):

- **Release and deployment planning:** plans for creating and deploying the release are created. This phase starts with Change Management authorization to plan a release and ends with Change Management authorization to create the release.
- **Release build and test:** the release package is built, tested, and checked into the DML. This phase starts with Change Management authorization to build the release and ends with Change Management authorization for the baselined release package to be checked into the DML by Service

- Asset and Configuration Management. This phase only happens once for each release.
- **Deployment:** the release package in the DML is deployed to the live environment. This phase starts with Change Management authorization to deploy the release package to one or more target environments and ends with handover to the service operation functions and early life support. There may be many separate deployment phases for each release, depending on the planned deployment options.
 - **Review and close:** experience and feedback are captured, performance targets and achievements are reviewed, and lessons are learned

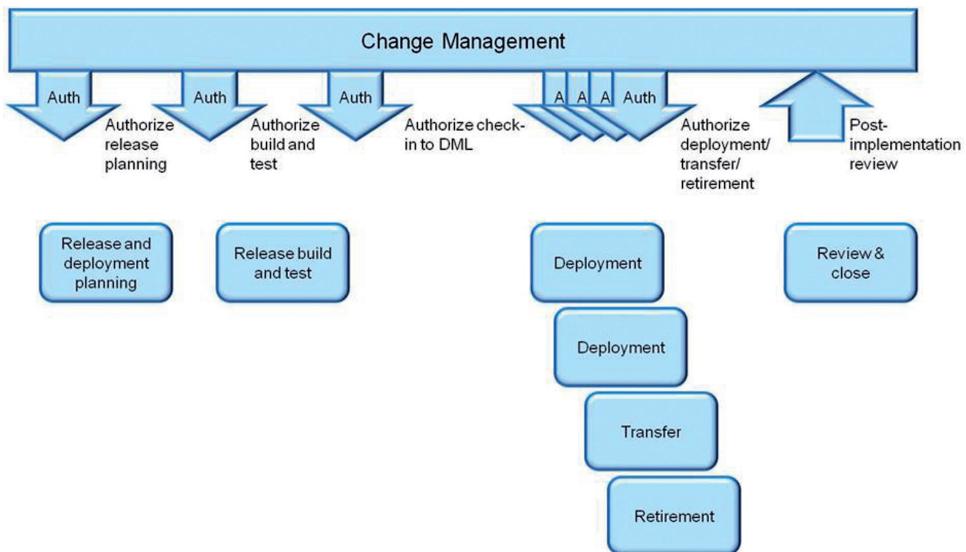


Figure 6.K—Relationship with Project Management

© Crown Copyright 2011 Reproduced under license from OGC

FIGURE 6.K SHOWS MULTIPLE POINTS where an authorized change triggers Release and Deployment Management activity. This does not require a separate RFC at each stage. Some organizations manage a whole release with a single change request and separate authorization at each stage for activities to continue, while other organizations require a separate RFC for each stage. Both of these approaches are acceptable; what is important is that Change Management authorization is received before commencing each stage.

Inputs

The inputs to Release and Deployment management are:

- Authorized change
- Service Design Package (SDP) including:
 - A service charter that defines the requirements from the business/customer for the service, including a description of the expected utility and warranty, as well as outline budgets and timescales
 - Service models that describe the structure and dynamics of how the service is operated and managed
 - Service acceptance criteria
 - IT service continuity plan and related business continuity plan
 - Service management and operations plans and standards
 - Technology and procurement standards and catalogues
 - Acquired service assets and components and their documentation
 - Build models and plans
 - Environment requirements and specifications for build, test, release, training, disaster recovery, pilot, and deployment
 - Release policy and release design from Service Design
 - Release and Deployment models including template plans
 - Exit and entry criteria for each stage of Release and Deployment Management

Outputs

The outputs from Release and Deployment Management are:

- New, changed, or retired services
- Release and deployment plan
- Updates to Change Management for the release and deployment activities
- Service notification
- Notification to Service Catalog Management to update the Service Catalog with the relevant information about the new or changed service

- New tested service capability and environment, including SLA, other agreements and contracts, changed organization, competent and motivated people, established business and service management processes, installed applications, converted databases, technology infrastructure, products, and facilities
- New or changed service management documentation
- SLA, underpinning OLAs, and contracts
- New or changed service reports
- Tested continuity plans
- Complete and accurate configuration item list with an audit trail for the CIs in the release package and also the new or changed service and infrastructure configurations
- Updated service capacity plan aligned to the relevant business plans
- Baseline release package—checked in to DML and ready for future deployments
- Service transition report

Service Transition Summary

EFFECTIVE SERVICE TRANSITION CAN SIGNIFICANTLY improve a Service Provider's ability to effectively handle high volumes of change and releases across its customer base. Other benefits delivered include:

- Increased success rate of changes and releases
- More accurate estimations of service levels and warranties
- Less variation of costs against those estimated in budgets
- Less variation from resources plans

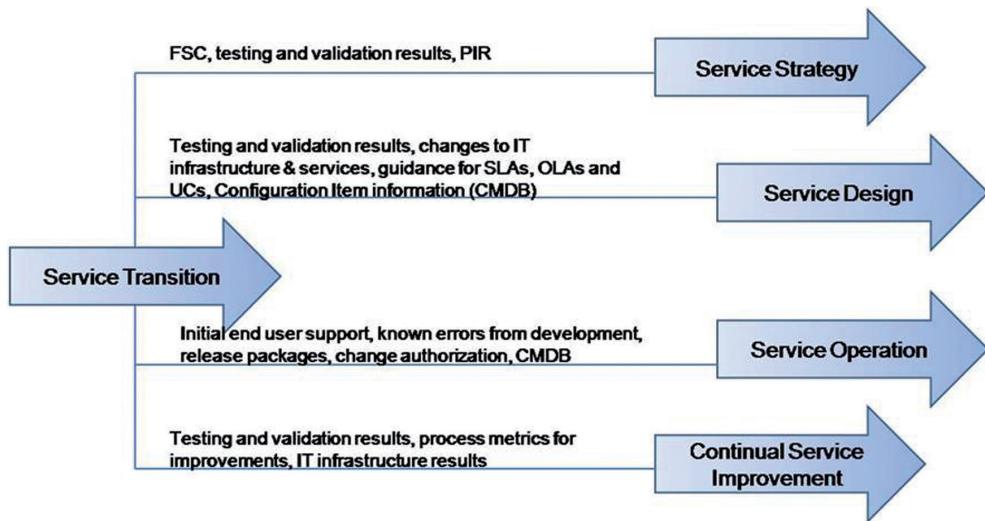


Figure 6.L —Some Service Transition Outputs to Other Lifecycle Stages

Service Transition Scenario

Transition Planning and Support

- Plan and coordinate the resources to ensure that the requirements are met
- Coordinate the activities across projects, suppliers, and service teams

Knowledge Management Considerations

- If your SKMS is established, you would be able to identify if you have the skills required to support videoconferencing, for example
- The SKMS will also help to determine the team required to build, test, and deploy HYPE
- Place to record and transfer user and support documentation

Service Asset and Configuration Management Considerations

- HYPE software is registered as a CI and relationships between it and the other CIs are known if/when an incident occurs. This will assist to speed up resolution times.
- Decision made as to whether webcams are CIs themselves or an attribute of the PC/laptop it is attached to

Change Management Considerations

- Ensure that the introduction of this new service minimizes impact on other services e.g., through testing, it is found that the RAM required slows down the PC, affecting other business critical apps. Change Management will assist with decision-making to determine the best path of action (through CAB).

Release and Deployment Management Considerations

- Builds and tests HYPE—decision here to limit video resolution to minimize bandwidth
- Stores original authorized software in DML
- Ensures that design aspects are adhered to when building (e.g., ensuring that the password policies are adhered to)
- Organizes training on using HYPE—priority given to Service Desk 1st and pilot users

Service Transition Review Questions

Question 1

The key element of a standard change is?

1. Documentation of a pre-approved procedure for implementing the change
2. Low risk to the production environment
3. No requirement for service downtime
4. It can be included in the next monthly or quarterly release

Question 2

The four phases of Release and Deployment are:

1. Release and deployment planning
2. Release build and test
- 3.
4. Review and close
 - Deployment

- » Change authorization
- » Change coordination
- » Release coordination

Question 3

The 4 spheres of Knowledge Management are:

1. Data, facts, knowledge, wisdom
2. Ideas, facts, knowledge, wisdom
3. Data, information, facts, wisdom
4. Data, information, knowledge, wisdom

Question 4

Which activity in Service Asset and Configuration Management would help to ascertain whether the recorded configuration items conform to the physical environment?

1. Control
2. Verification and audit
3. Identification
4. Status accounting

Question 5

After a change has been implemented, an evaluation is performed. What is this evaluation called?

1. Forward Schedule of Changes (FSC)
2. Post Implementation Review (PIR)
3. Service Improvement Program (SIP)
4. Service Level Requirement (SLR)

Question 6

Which of the following is not a change type?

1. Standard change
2. Normal change
3. Quick change
4. Emergency change

Question 7

Which process is responsible for maintaining software items in the Definitive Media Library (DML)?

1. Release and Deployment Management
2. Service Asset and Configuration Management
3. Service validation and testing
4. Change Management

Question 8

Which process or function is responsible for communicating the change schedule to the users?

1. Change Management
2. Service Desk
3. Release and Deployment Management
4. Service Level Management

Question 9

Which of the following best describes a baseline?

1. Used as a reference point for later comparison
2. The starting point of any project
3. The end point of any project
4. A rollback procedure

Question 10

The main objective of Change Management is to?

1. Ensure that any changes are approved and recorded
2. Ensure that standardized methods and procedures are used for controlled handling of all changes
3. Ensure that any change requests are managed through the CAB
4. Ensure that the CAB takes responsibility for all change implementation

Chapter 7

SERVICE OPERATION

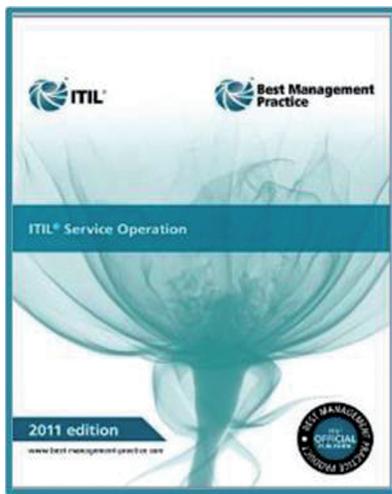


Figure 7.A—Service Operation

Purpose

The primary purpose of the Service Operation stage of the Service Lifecycle is to coordinate, deliver, and manage services to ensure that the levels agreed with the business, customers, and users are met or exceeded. Service Operation is also responsible for the ongoing management of the technology that is used to deliver and support the services.

Service Operation accepts the new, modified, retiring, or retired services from Service Transition, once the test and acceptance criteria have been met. Service Operation then ensures that those new or modified services will meet all of their agreed operational targets, as well as ensuring that all existing services continue to meet all of their targets. This stage of the lifecycle performs the vital day-to-day activities and processes that collect the data and information that are essential to the activities of Continual Service Improvement, the final stage of the Service Lifecycle.

Service Operation is the critical stage of the Service Lifecycle. It is the stage of the lifecycle where the service really starts to deliver benefit and value to the business, customers, and users. A well-designed and implemented service and its processes will be of little value if they are poorly supported, operated, and managed. Service Operation staff should have in place effective processes with supporting tools to allow them an overall view of the service and service operation (rather than just the separate components, such as hardware, software applications, and networks). This will enable them to rapidly detect any threats or failures to the service and service quality. Service Operation staff act as the 'eyes and ears' for the service provider organization, 24 hours a day, seven days a week, giving early warning of any abnormal situations, especially on mission-critical services.

The objectives of Service Operation are to:

- Maintain business satisfaction and confidence in IT through effective and efficient delivery and support of agreed IT services
- Minimize the impact of service outages on day-to-day business activities
- Ensure that access to agreed IT services is only provided to those authorized to receive those services

Value to the business

SELECTING AND ADOPTING THE BEST practice as recommended in this publication will assist organizations in delivering significant benefits. Adopting and implementing standard and consistent approaches for Service Operation will:

- Reduce unplanned labor and costs for both the business and IT through optimized handling of service outages and identification of their root causes
- Reduce the duration and frequency of service outages, which will allow the business to take full advantage of the value created by the services they are receiving
- Provide operational results and data that can be used by other ITIL® processes to improve services continually and provide justification for investing in ongoing service improvement activities and supporting technologies

- Meet the goals and objectives of the organization's security policy by ensuring that IT services will be accessed only by those authorized to use them
- Provide quick and effective access to standard services, which business staff can use to improve their productivity or the quality of business services and products
- Provide a basis for automated operations, thus increasing efficiencies and allowing expensive human resources to be used for more innovative work, such as designing new or improved functionality or defining new ways in which the business can exploit technology for increased competitive advantage

Major Concepts

Achieving the Balance

SERVICE OPERATION IS MORE THAN just a repetitive execution of a standard set of procedures or activities; this stage works in an ever-changing environment. One of Service Operation's key roles is dealing with the conflict between maintaining the status quo, adapting to the changing business and technological environments, and achieving a balance between conflicting sets of priorities.

Internal IT View:

Focuses on the way in which IT components and systems are managed to deliver the services. An organization here is out of balance and is in danger of not meeting business requirements.

Stability:

No matter how good the functionality is of an IT service or how well it has been designed, it will be worth far less if the service components are not available or if they perform inconsistently. Service Operation has to ensure that the IT infrastructure is stable and available as required. However an extreme focus on stability means that IT is in danger of ignoring changing business requirements

VS

External Business View:

Focuses on the way in which services are experienced by users and customers. An organization has business focus, but tends to under-deliver on promises to the business.

Responsiveness:

Service Operation must recognize that the business and IT requirements change.

VS

When there is an extreme focus on responsiveness IT may tend to overspend on change and also decrease the stability of the infrastructure.

Cost of Service:

An organization with an extreme focus on cost is out of balance and is in danger of losing service quality because of heavy cost cutting. The loss of service quality leads to a loss of customers, which in turn leads to further cost cutting as the negative cycle continues.

VS

Quality of Service:

An organization with an extreme focus on quality has happy customers but may tend to overspend to deliver higher levels of service than are strictly necessary, resulting in higher costs and effort required.

The goal should be to consistently deliver the agreed level of IT service to customer and users, while at the same time keeping costs and resource utilization at an optimal level.

Reactive:

An organization that is extremely reactive is not able to effectively support the business strategy. Unfortunately a lot of organizations focus on reactive management as the sole means of ensuring that services are highly consistent and stable, actively discouraging proactive behavior from staff. The worst aspect of this approach is that discouraging effort investment in proactive service management can ultimately increase the effort and cost of reactive activities and further risk stability and consistency in services.

VS

Proactive:

An extremely proactive organization tends to fix services that are not broken or introduce services that are not yet needed, resulting in higher levels of change, cost, and effort.

This also comes at a cost to the stability of the infrastructure and quality of service already being delivered.

Service Operation Functions

"Know your role, do your job"

TEAM MOTTO DESCRIBING THE GOAL for every player, coach, and general staff member of the Kansas City Chiefs.

Functions refer to the people (or roles) and automated measures that execute a defined process, an activity, or combination of both. The functions within Service Operation are needed to manage the 'steady state' operation IT environment. Just like in sports where each player will have a specific role to play in the overall team strategy, IT functions define the different roles and responsibilities required for the overall service delivery and support of IT services.

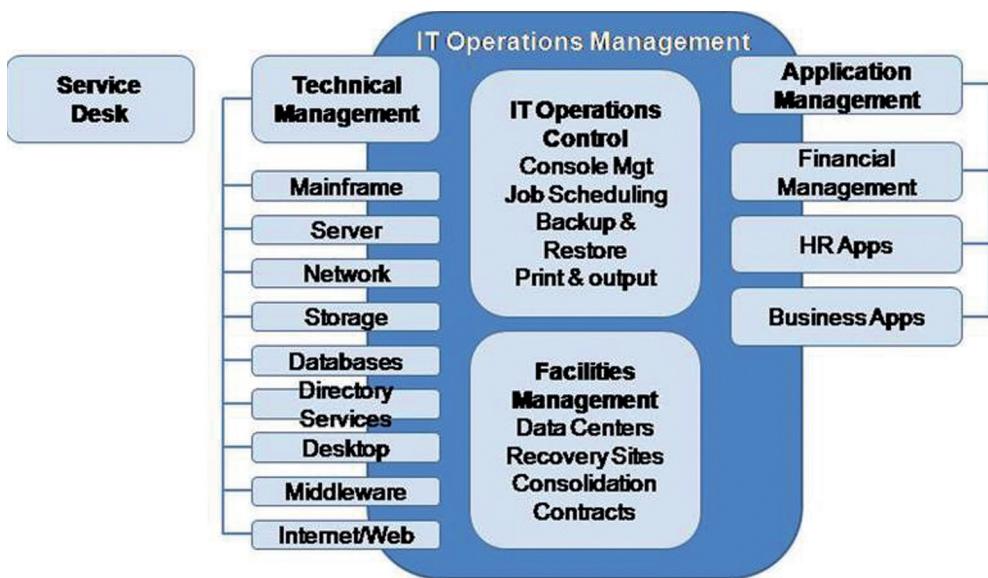


Figure 7.B—The ITIL® Functions from Service Operation

NOTE: THESE ARE LOGICAL FUNCTIONS and do not necessarily have to be performed by equivalent organizational structure. This means that Technical and Application Management can be organized in any combination and into any number of departments. The lower groupings (e.g., Mainframe, Server) are examples of activities performed by Technical Management and are not a suggested organizational structure.

The Service Desk

Purpose

THE PRIMARY AIM OF THE Service Desk is to provide a single point of contact between the services being provided and the users. A typical Service Desk manages incidents and service requests and also handles communication with the users. Service Desk staff execute the Incident Management and Request Fulfillment processes to restore the normal-state service operation to the users as quickly as possible. In this context ‘restoration of service’ is meant in the widest possible sense. While this could involve fixing a technical fault, it could equally involve fulfilling a service request or answering a query—anything that is needed to allow the users to return to working satisfactorily.

Specific responsibilities will include:

- Logging all relevant incident/service request details, allocating categorization and prioritization codes
- Providing first-line investigation and diagnosis
- Resolving incidents/service requests when first contacted, whenever possible
- Escalating incidents/service requests that they cannot resolve within agreed timescales
- Keeping users informed of progress
- Closing all resolved incidents, requests, and other calls
- Conducting customer/user satisfaction call-backs/surveys as agreed
- Communication with users—keeping them informed of incident progress, notifying them of impending changes or agreed outages, etc.
- Updating the CMS under the direction and approval of Service Asset and Configuration Management, if so agreed.

Service Desk Organizational Structures

MANY FACTORS WILL INFLUENCE THE way in which a Service Desk function will be physically structured, such as the location, languages and cultures of end users, diversity in services and technology supported, and the objectives governing the implementation of the Service Desk, such as improved satisfaction or reduced operating costs.

The following are some of the main options chosen when implementing a Service Desk function:

Local Service Desk

A local Service Desk structure is where the Service Desk is co-located within or physically close to the user community it serves. This may aid in communication and give the Service Desk a visible presence, which some users may like. It may, however, be inefficient and expensive to have multiple Service Desks operating.

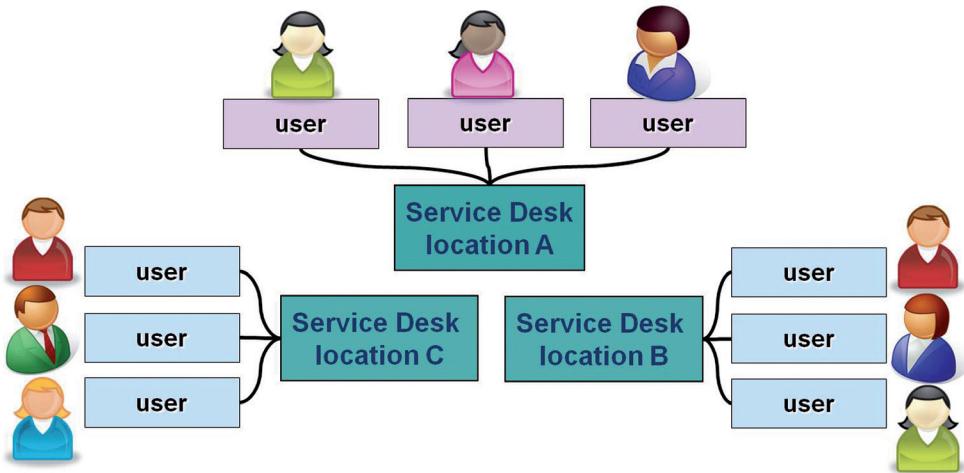


Figure 7.C—The Local Service Desk Structure

Benefits of a local Service Desk structure	Disadvantages of a local Service Desk structure
<ul style="list-style-type: none">• Local and specific user knowledge• Ability to effectively communicate with multiple languages• Appropriate cultural knowledge• Visible (and physical) presence of the Service Desk	<ul style="list-style-type: none">• Higher costs for replicated infrastructure and more staff involved• Less knowledge transfer, each Service Desk may spend time rediscovering knowledge• Inconsistency in service levels and reporting• Service Desks may be focused on local issues

Centralized Service Desk

A centralized structure uses a Service Desk in a single location (or smaller number of locations), although some local presence may remain to handle physical support requirements, such as deploying, moving, and disposing of user workstations. This could be more efficient, enabling less staff to manage a higher volume of calls with greater visibility of repeat incidents and requests.

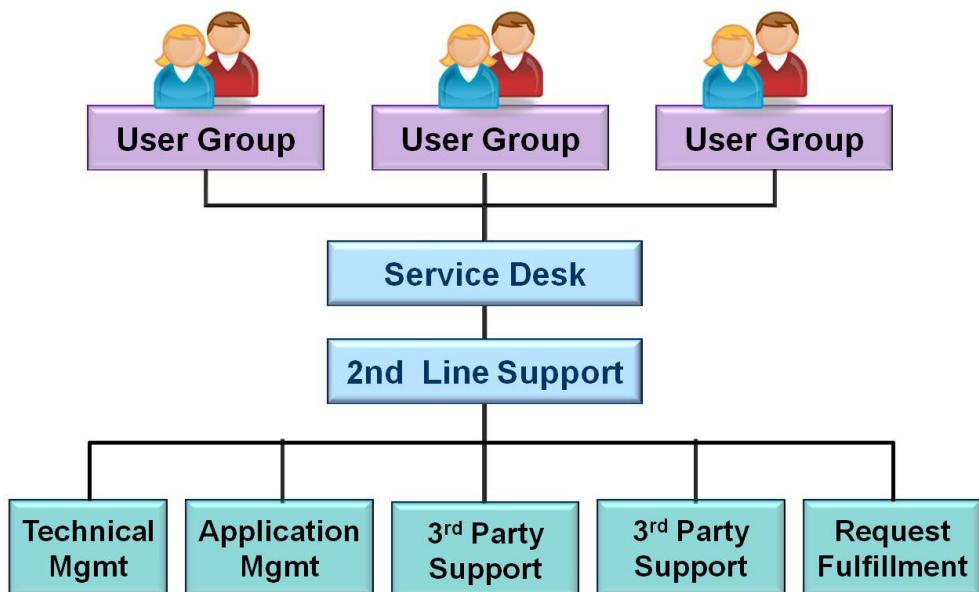


Figure 7.D—The Centralized Service Desk Structure

Benefits of a centralized Service Desk structure	Disadvantages of a centralized Service Desk structure
<ul style="list-style-type: none">• Reduced operational costs• Improved usage of available resources• Consistency of call handling• Improved ability for knowledge sharing• Simplicity for users (call one number) to contact the Service Desk	<ul style="list-style-type: none">• Potentially higher costs and challenges in handling 24x7 environment or different time zones• Lack of local knowledge• Possible gaps in language and culture• Higher risk (single point of failure), in case of power loss or other physical threat

Virtual Service Desk

A virtual Service Desk, through the use of technology, particularly the Internet, and the use of corporate support tools, can give users the impression of a single, centralized Service Desk when, in fact, the personnel may be spread or located in any number of geographical or structural locations.

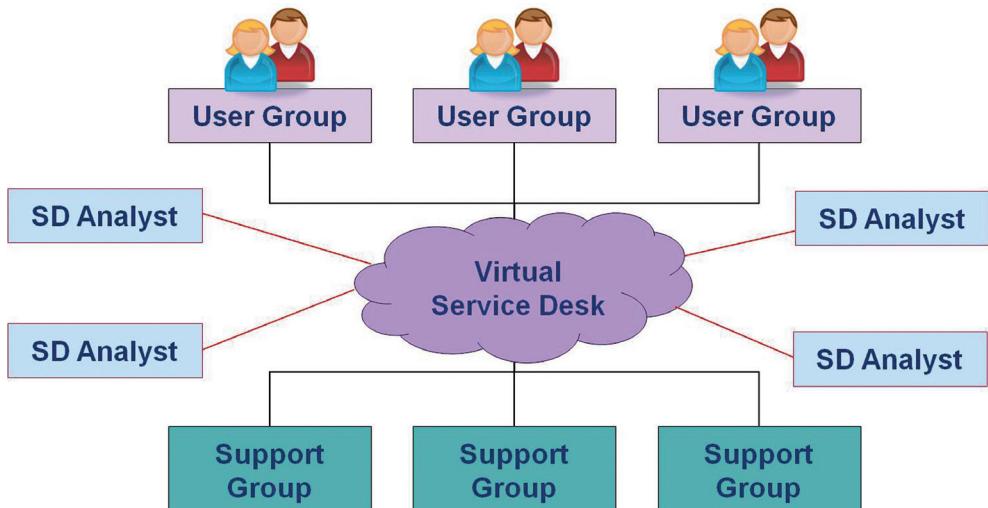


Figure 7.E—A Virtual Service Desk Structure

Benefits of a virtual Service Desk structure	Disadvantages of a virtual Service Desk structure
<ul style="list-style-type: none">• Support for global organizations• 24x7 support in multiple time zones• Reduced operational costs• Improved usage of available resources• Effective matching of appropriate staff for different types of calls	<ul style="list-style-type: none">• Initial cost of implementation, requiring diverse and effective voice technology• Lack in the consistency of service and reporting• Less effective for monitoring actions of staff• Staff may feel disconnected from other Service Desk staff

Follow the Sun

Some global or international organizations will combine two or more of their geographically dispersed Service Desks to provide 24-hour follow-the-sun service.



Figure 7.F—A Follow-the-Sun Service Desk structure

Benefits of a follow-the-sun Service Desk structure	Disadvantages of a follow-the-sun Service Desk structure
<ul style="list-style-type: none">• Support for global organizations• 24x7 support in multiple time zones• Improved quality of service• Improved customer/user satisfaction• Effective knowledge sharing and high level visibility of distributed infrastructure	<ul style="list-style-type: none">• Typically higher operating costs• Cost of required technology• Challenges in using single language for multiple regions when recording knowledge, workarounds, Known Errors etc.

Skills

Due to the role played by the Service Desk, staff members need to have (or have the ability to develop):

- Communication Skills
- Technical Skills
- Business Understanding

The most important of these three areas is communication skills, as the primary role of the Service Desk is to provide a Single Point of Contact between the end-users and the IT organization. Because of this, they will need to be able to deal effectively with a wide range of people and situations.

Staff Retention

To ensure a balanced mix of experienced and newer staff, Service Desk managers should use a number of methods and incentives to retain quality staff and to avoid disruption and inconsistency in the quality of support offered.

Some ways in which this can be done include:

- Recognition of staff achievements contributing to service quality
- Rotation of staff onto other activities (projects, second-line support, etc.)
- Team building exercises and celebrations
- Promoting the Service Desk as a potential stepping stone for staff to move into other more technical or supervisory roles (after defined time periods and skills achieved)

Self help

MANY ORGANIZATIONS FIND IT BENEFICIAL to offer self-help capabilities to their users. The technology should, therefore, support this capability, with the web front-end allowing web pages to offer a menu-driven range of self help and service requests—with a direct interface into the back-end process-handling software. This reduces the amount of calls into the Service Desk and is often used as a source for improvements to efficiency. An example of this is the ability for a customer to track the status of their parcels online when shipped through a major courier company.

Aside from this, the Service Desk will use many different tools, systems, and other technology components in order to provide effective and efficient support to end-user calls and requests. To enable this, typical technology components utilized include:

- Computerized Service Desk systems
- Voice services (adv. menu systems, voicemail, SMS)
- Web and email (access, notification, updates)
- Systems that contain linkages to SLAs, CMDB
- Access to availability monitoring tools
- Self help for customers using technology
- Service Desk Metrics

To evaluate the true performance of the Service Desk, a balanced range of metrics should be established and reviewed at regular intervals. Especially dangerous is the tendency to focus on “average call time” or “number of calls answered” metrics, which can mask underlying issues with the quality of support provided.

Some of the typical metrics reviewed when monitoring the performance of the Service Desk include:

- The number of calls to Service Desk (broken down by type and work period)
- First-line resolution rate

- Average Service Desk cost of handling any incident or request
- Number of knowledgebase articles created
- Number or percentage of SLA breaches
- Call resolution time
- Customer satisfaction (surveys)
- Use of self help (where exists)

Outsourcing the Service Desk

ALTHOUGH FAIRLY COMMON, THERE ARE potential risks that can be introduced when outsourcing an organization's Service Desk. When reviewing the potential for this to occur, service managers should consider the following items when developing contracts to reduce these risks:

- Use of your own service management tool, not theirs
- Retain ownership of data
- Ability to maintain required staffing levels
- Agreements on reporting and monitoring needs
- Proven up-to-date procedures
- Agreed and understood support needs
- Engage contract specialists for assistance

Technical Management

TECHNICAL MANAGEMENT REFERS TO THE groups, departments, or teams that provide technical expertise and overall management of the IT infrastructure.

The objectives of Technical Management are to help plan, implement, and maintain a stable technical infrastructure to support the organization's business processes through:

- Well-designed and highly resilient, cost-effective technical topology
- The use of adequate technical skills to maintain the technical infrastructure in optimum condition
- Swift use of technical skills to speedily diagnose and resolve any technical failures that do occur

Technical Management plays a dual role:

- It is the custodian of technical knowledge and expertise related to managing the IT infrastructure. In this role, Technical Management ensures that the knowledge required to design, test, manage, and improve IT services is identified, developed, and refined
- It provides the actual resources to support the Service Lifecycle. In this role, Technical Management ensures that resources are effectively trained and deployed to design, build, transition, operate, and improve the technology required to deliver and support IT services

By performing these two roles, Technical Management is able to ensure that the organization has access to the right type and level of human resources to manage technology and, thus, to meet business objectives.

Part of this role is also to ensure a balance between the skill level, utilization, and cost of these resources. For example, hiring a top-level resource at the higher end of the salary scale and then only using that skill for 10% of the time is not effective. A better Technical Management strategy would be to identify the times that the skill is needed and then hire a contractor for only those tasks.

Another strategy in larger organizations is to leverage specialist staff out of central pools so that specialists can be well-utilized and provide an economy of scale to the organization, minimizing the need to hire in contractors. Specialized skills should be identified among resources in the IT organization and then leveraged for specific needs as they arise, analogous to a special tactical unit whose members also perform regular duties but who are assigned to tasks needing their specialized skills. This type of resource utilization is particularly useful both for project teams and problem resolution.

An additional but very important role played by Technical Management is to provide guidance to IT operations about how best to carry out the ongoing operational management of technology. This role is partly carried out during the Service Design process, but it is also a part of everyday communication with IT Operations Management as they seek to achieve stability and optimum performance.

One or more technical support teams or departments will be needed to provide Technical Management and support for the IT Infrastructure.

In all but the smallest organizations where a single combined team or department may suffice, separate teams or departments will be needed for each type of infrastructure being used. In many organizations the Technical Management (TM) departments are also responsible for the daily operation of a subset of the IT Infrastructure.

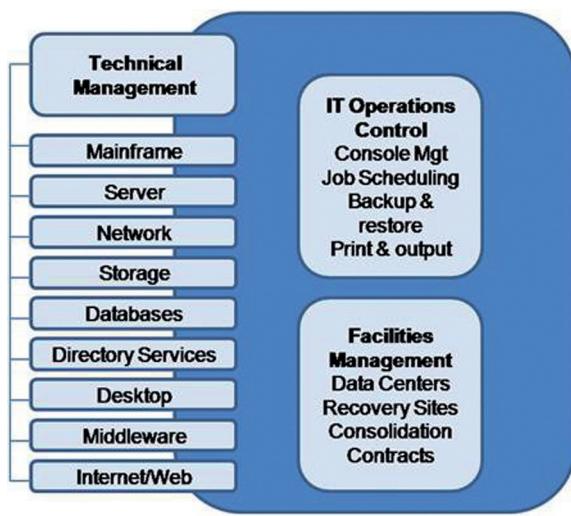


Figure 7.G—Technical Management

In many organizations, the actual role played by IT Operations Management is carried out by either Technical or Application Management.

Roles and Responsibilities

- Custodian of technical knowledge and expertise related to managing the IT Infrastructure. Provides detailed technical skills and resources needed to support the ongoing operation of the IT Infrastructure.
- Plays an important role in providing the actual resources to support the IT Service Management lifecycle. Ensures resources are effectively trained and deployed to design, build, transition, operate, and improve the technology to deliver and support IT Services.



Figure 7.H—Staff making up the Technical Management Function

To **ENABLE QUALITY KNOWLEDGE SHARING** and continual improvement of services, technology, processes, and other capabilities, Technical Management staff should develop effective communication channels and meet regularly to discuss issues or potential ideas. History demonstrates that quality design requires involvement from those who will be supporting the product/service, as does quality support require involvement from the designers in turn.

IT Operations Management

IN BUSINESS, THE TERM ‘OPERATIONS management’ is used to mean the department, group, or team of people responsible for performing the organization’s day-to-day operational activities—such as running the production line in a manufacturing environment or managing the distribution centers and fleet movements within a logistics organization.

Operations Management generally has the following characteristics:

- There is work to ensure that a device, system, or process is actually running or working (as opposed to strategy or planning)
- This is where plans are turned into actions
- The focus is on daily or shorter-term activities; although, it should be noted that these activities will generally be performed and repeated over a relatively long period (as opposed to one-off project-type activities)
- These activities are executed by specialized technical staff who often have to undergo technical training to learn how to perform each activity
- There is a focus on building repeatable, consistent actions that, if repeated frequently enough at the right level of quality, will ensure the success of the operation
- This is where the actual value of the organization is delivered and measured
- There is a dependency on investment in equipment or human resources or both
- The value generated must exceed the cost of the investment and all other organizational overheads (such as management and marketing costs) if the business is to succeed

In a similar way, IT Operations Management can be defined as the function responsible for the ongoing management and maintenance of an organization’s IT infrastructure to ensure delivery of the agreed level of IT services to the business.

IT operations can be defined as the set of activities involved in the day-to-day running of the IT infrastructure for the purpose of delivering IT services at agreed levels to meet stated business objectives.

In some organizations this is a single, centralized department, while in others some activities and staff are centralized and some are provided by distributed and specialized departments.

In many cases, the role of IT Operations Management is actually performed by the Technical and Application Management functions, where required.

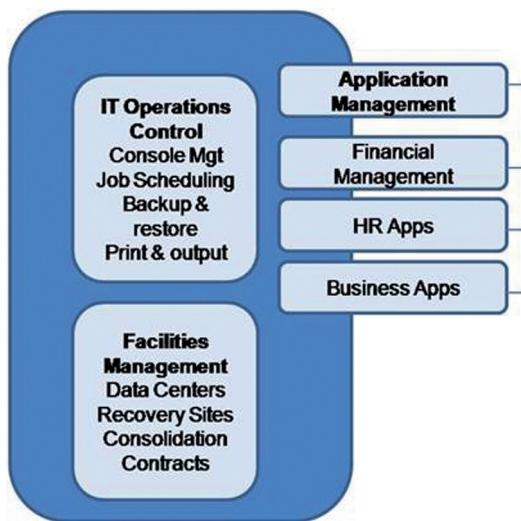


Figure 7.1—IT Operations Management

IT Operations Control

ONE ROLE PLAYED BY IT Operations Management is that of Operations Control. This role is concerned with the execution and monitoring of the operational activities and events in the IT infrastructure (possibly using an Operations/Network Bridge). In addition to the routine tasks to be performed in accordance with the design specifications of the IT infrastructure, Operations Control is also responsible for the following:

- Console management/operations bridge, which refers to defining central observation and monitoring capability and then using those consoles to exercise event management, monitoring, and control activities
- Job scheduling or the management of routine batch jobs or scripts
- Backup and restore on behalf of all Technical and Application Management teams and departments and often on behalf of users
- Print and output management for the collation and distribution of all centralized printing or electronic output

- Performance of maintenance activities on behalf of Technical or Application Management teams or departments

Facilities Management

FACILITIES MANAGEMENT REFERS TO THE role responsible for management of all physical IT environments, usually data centers, computer rooms, and recovery sites. In some organizations, many physical components have been outsourced and Facilities Management may include the management of the outsourcing contracts. For any organization, this is a very important element of IT Service Management and will contribute to the ability to provide a safe working environment. Facilities Management should be involved in any large scale project planning to provide advice regarding any physical accommodation of staff or infrastructure required.

Application Management

APPLICATION MANAGEMENT IS RESPONSIBLE FOR managing applications throughout their lifecycle. This differs from application development as Application Management covers the entire ongoing lifecycle of an application, including requirements, design, build, deploy, operate, and optimize. The Application Management function is performed by any department, group, or team involved in managing and supporting operational applications. Application Management also plays an important role in the design, testing, and improvement of applications that form part of IT services. As such, it may be involved in development projects but is not usually the same as the application development teams.

The objectives of Application Management are to support the organization's business processes by helping to identify functional and manageability requirements for application software and then to assist in the design and deployment of those applications and the ongoing support and improvement of those applications.

These objectives are achieved through:

- Applications that are well-designed, resilient, and cost-effective
- Ensuring that the required functionality is available to achieve the required business outcome
- The organization of adequate technical skills to maintain operational applications in optimum condition
- Swift use of technical skills to speedily diagnose and resolve any technical failures that do occur

Roles and Responsibilities

APPLICATION MANAGEMENT IS TO APPLICATIONS what Technical Management is to the IT infrastructure. Application Management activities are performed in all applications, whether purchased or developed in-house. One of the key decisions that they contribute to is the decision of whether to buy an application or build it (this is discussed in detail in *ITIL® Service Design*). Once that decision is made, Application Management will have several roles:

- It is the custodian of technical knowledge and expertise related to managing applications. In this role, Application Management, working together with Technical Management, ensures that the knowledge required to design, test, manage, and improve IT services is identified, developed, and refined.
- It provides the actual resources to support the Service Lifecycle. In this role, Application Management ensures that resources are effectively trained and deployed to design, build, transition, operate, and improve the technology required to deliver and support IT services.

Application Management also performs other specific roles:

- Providing guidance to IT operations about how best to carry out the ongoing operational management of applications. This role is partly carried out during the Service Design process, but it is also a part of everyday communication with IT Operations Management as they seek to achieve stability and optimum performance.
- The integration of the Application Management lifecycle into the service lifecycle

Application Management Lifecycle

APPLICATION DEVELOPMENT PROCESSES SHOULD BE implemented as part of a coordinated approach to IT Service Management, although, in many cases, this fails to happen. When the development of applications is not integrated with the rest of ITSM, it often leads to a breakdown in communication channels between developers and support staff and, ultimately, releasing applications that are not optimal in supporting business processes.

Application development and operations are part of the same overall lifecycle and both should be involved at all stages, although their level of involvement will vary depending on the stage of the lifecycle.

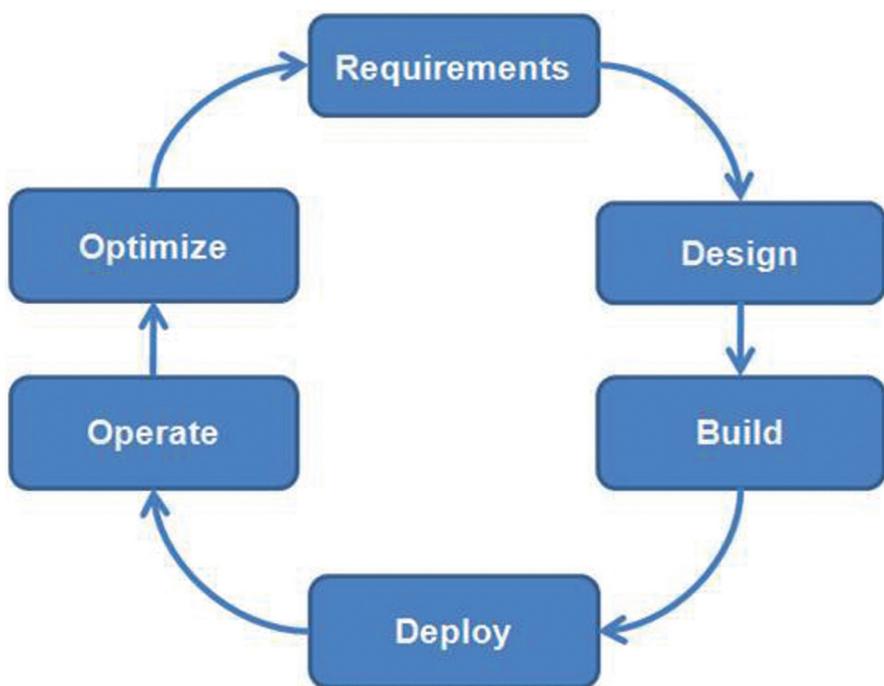


Figure 7.K—The Application Management Lifecycle

© Crown Copyright 2011 Reproduced under license from OGC

Service Operation Processes

THE GOAL OF SERVICE OPERATION, as previously mentioned, is to enable effectiveness and efficiency in delivery and support of IT services. The processes that support this goal are:

- Event Management
- Incident Management
- Problem Management
- Request Fulfillment
- Access Management

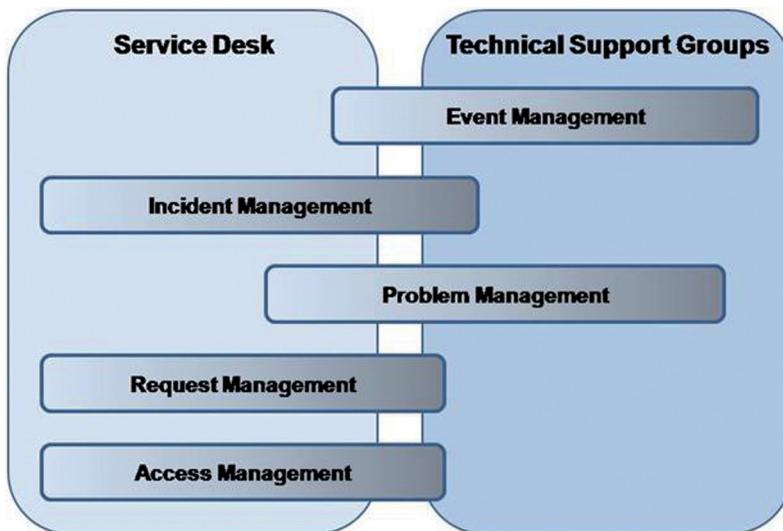


Figure 7.1—Where the Service Operation Processes Get Carried Out

THE FIGURE ABOVE DEMONSTRATES HOW much responsibility the Service Desk and the technical support groups (Technical, IT Operations, and Application Management functions) have in the Service Operation Processes. Incident Management, Request Fulfillment, and Access Management are primarily carried out by the Service Desk, with Event Management and Problem Management as primarily back-of-house processes.

Event Management

Terminology

Term	Definition
alert	(ITIL® Service Operation) A notification that a threshold has been reached, something has changed, or a failure has occurred. Alerts are often created and managed by system management tools and are managed by the event management process.
event	(ITIL® Service Operation) A change of state that has significance for the management of an IT service or other configuration item. The term is also used to mean an alert or notification created by any IT service, configuration item, or monitoring tool. Events typically require IT operations personnel to take actions and often lead to incidents being logged.

Purpose

THE PURPOSE OF **EVENT MANAGEMENT** is to manage events throughout their lifecycle. This lifecycle of activities to detect events, make sense of them, and determine the appropriate control action is coordinated by the Event Management process.

Event Management is, therefore, the basis for operational monitoring and control. If events are programmed to communicate operational information, as well as warnings and exceptions, they can be used as a basis for automating many routine operations management activities, for example, executing scripts on remote devices or submitting jobs for processing, or even dynamically balancing the demand for a service across multiple devices to enhance performance.

The objectives of the Event Management process are to:

- Detect all changes of state that have significance for the management of a CI or IT service
- Determine the appropriate control action for events and ensure these are communicated to the appropriate functions
- Provide the trigger, or entry point, for the execution of many service operation processes and operations management activities
- Provide the means to compare actual operating performance and behavior against design standards and SLAs

- Provide a basis for service assurance and reporting and service improvement (This is covered in detail in ITIL® Continual Service Improvement)

Scope

EVENT MANAGEMENT CAN BE APPLIED to any aspect of service management that needs to be controlled and can be automated. This includes:

- Configuration items (CIs):
 - Some CIs will be included because they need to stay in a constant state (e.g., a switch on a network needs to stay on and event management tools confirm this by monitoring responses to pings)
- Some CIs will be included because their status needs to change frequently and Event Management can be used to automate this and update the Configuration Management System (CMS) (e.g., the updating of a file server)
- Environmental conditions (e.g., fire and smoke detection)
- Software license monitoring for usage to ensure optimum/legal license utilization and allocation
- Security (e.g., intrusion detection)
- Normal activity (e.g., tracking the use of an application or the performance of a server)

Types of events

THERE ARE MANY DIFFERENT TYPES of events, such as informational events, warning events, and exception events

Informational events

- A scheduled workload has completed
- A user has logged in to use an application
- An email has reached its intended recipient

Warning events

- A server's memory utilization reaches within 5% of its highest acceptable performance level
- The completion time of a transaction is 10% longer than normal

Warning events signify unusual but not exceptional operation. These are an indication that the situation may require closer monitoring. In some cases, the condition will resolve itself, for example, in the case of an unusual combination of workloads—as they are completed, normal operation is restored. In other cases, operator intervention may be required if the situation is repeated or if it continues for too long. These rules or policies are defined in the monitoring and control objectives for that device or service.

Exception events

- A user attempts to log on to an application with the incorrect password
- An unusual situation has occurred in a business process that may indicate an exception requiring further business investigation (e.g., a web page alert indicates that a payment authorization site is unavailable, impacting financial approval of business transactions)
- A device's CPU is above the acceptable utilization rate
- A PC scan reveals the installation of unauthorized software

Two things are significant about the above examples:

- Exactly what constitutes informational versus a warning versus an exception? There is no definitive rule about this. Informational events convey data for use in decision-making, warning events tend to convey predictive information that some exception might occur, and exception events indicate an abnormal situation that requires action to address. For example, a manufacturer may provide information that a benchmark of 75% memory utilization is optimal for application X. However, it is discovered that, under specific conditions, response times begin to degrade above 70% utilization. Thresholds are then set, which trigger warning events if utilization is between 70 and 75%. At 75% or higher, an exception event is triggered that will require immediate action, such as adding more memory.
- Each relies on the sending and receipt of a message of some sort. These are generally referred to as event notifications and they do

not just happen without planning. The following sections will explore exactly how events are defined, generated and captured.

One of the most important principles of Event Management is achieving the correct level of filtering to focus management and control actions on those events that have significance. This can become complicated by the fact that the significance of events changes. For example, a user logging into a system today is normal, but, if that user leaves the organization and tries to log in, it is a security breach.

Inputs

Inputs to the Event Management process will mostly come from Service Design and Service Transition. Examples of these may include:

- Operational and service level requirements associated with events and their actions
- Alarms, alerts, and thresholds for recognizing events
- Event correlation tables, rules, event codes, and automated response solutions that will support Event Management activities
- Roles and responsibilities for recognizing events and communicating them to those that need to handle them
- Operational procedures for recognizing, logging, escalating, and communicating events

Outputs

EXAMPLES OF OUTPUTS FROM EVENT Management may include:

- Events that have been communicated and escalated to those responsible for further action
- Event logs describing what events took place and any escalation and communication activities taken to support forensic, diagnosis, or further CSI activities
- Events that indicate an incident has occurred
- Events that indicate the potential breach of an SLA or OLA objective
- Events and alerts that indicate completion status of deployment, operational, or other support activities
- Populated SKMS with event information and history

Incident Management

INCIDENT MANAGEMENT HAS DEVELOPED OVER time to become one of the most visible and mature ITIL® processes for any organization, largely driven by the need to reduce the business impact of disruptions to IT services. While any effective implementation does balance the efforts towards the various stages of the Service Lifecycle, as Incident Management can be easily demonstrated to have a business benefit, it typically receives more attention and funding than other areas of service management. This section will explain the activities and techniques that represent best practices for Incident Management.

In ITIL® terminology, an incident is defined as an unplanned interruption to an IT service or reduction in the quality of an IT service or a failure of a CI that has not yet impacted an IT service. Incident Management is the process responsible for managing the lifecycle of all incidents. Incidents may be recognized by technical staff, detected and reported by event monitoring tools, communications from users (usually via a telephone call to the Service Desk), or reported by third-party suppliers and partners.

Terminology

Term	Definition
escalation	(ITIL® Service Operation) An activity that obtains additional resources when these are needed to meet service level targets or customer expectations. Escalation may be needed within any IT service management process but is most commonly associated with incident management, problem management, and the management of customer complaints. There are two types of escalation: functional escalation and hierarchic escalation.
functional escalation	(ITIL® Service Operation) Transferring an incident, problem, or change to a technical team with a higher level of expertise to assist in an escalation.
hierarchic escalation	(ITIL® Service Operation) Informing or involving more senior levels of management to assist in an escalation.
impact	(ITIL® Service Operation) (ITIL® Service Transition) A measure of the effect of an incident, problem, or change on business processes. Impact is often based on how service levels will be affected. Impact and urgency are used to assign priority.

Term	Definition
incident	(ITIL® Service Operation) An unplanned interruption to an IT service or reduction in the quality of an IT service. Failure of a configuration item that has not yet affected service is also an incident—for example, failure of one disk from a mirror set.
incident record	(ITIL® Service Operation) A record containing the details of an incident. Each incident record documents the lifecycle of a single incident.
major incident	(ITIL® Service Operation) The highest category of impact for an incident. A major incident results in significant disruption to the business.
resolution	(ITIL® Service Operation) Action taken to repair the root cause of an incident or problem or to implement a workaround. In ISO/IEC 20000, resolution processes is the process group that includes incident and problem management.
restore	(ITIL® Service Operation) Taking action to return an IT service to the users after repair and recovery from an incident. This is the primary objective of incident management.
urgency	(ITIL® Service Design) (ITIL® Service Transition) A measure of how long it will be until an incident, problem, or change has a significant impact on the business. For example, a high-impact incident may have low urgency if the impact will not affect the business until the end of the financial year. Impact and urgency are used to assign priority.
workaround	(ITIL® Service Operation) Reducing or eliminating the impact of an incident or problem for which a full resolution is not yet available—for example, by restarting a failed configuration item. Workarounds for problems are documented in known error records. Workarounds for incidents that do not have associated problem records are documented in the incident record.

Purpose

THE PURPOSE OF **INCIDENT MANAGEMENT** is to restore normal service operation as quickly as possible and minimize the adverse impact on business operations, thus, ensuring that agreed levels of service quality are maintained. Normal service operation is defined as an operational state where services and CIs are performing within their agreed service and operational levels. It is defined as operating within the agreed Service Level Agreement (SLA) limits.

The objectives of the Incident Management process are to:

- Ensure that standardized methods and procedures are used for efficient and prompt response, analysis, documentation, ongoing management, and reporting of incidents
- Increase visibility and communication of incidents to business and IT support staff
- Enhance business perception of IT through use of a professional approach in quickly resolving and communicating incidents when they occur
- Align Incident Management activities and priorities with those of the business
- Maintain user satisfaction with the quality of IT services

What is the difference between Incident Management and Problem Management?

If our garden had weeds, how would we address the situation?

Incident Management: Use techniques that address the symptoms but still allow the weeds to grow back (e.g., pull them out, mow over them, use a hedge-trimmer, or buy a goat)

Problem Management: Use techniques that address the root-cause of the symptoms so that weeds will no longer grow (e.g., use poison, dig roots out, re-lawn, concrete over, etc.)

Incident Management is not concerned with the root cause; it is instead focused on addressing the symptoms as quickly as possible.

Scope

INCIDENT MANAGEMENT CAN BE UTILIZED to manage any event that disrupts or has the potential to disrupt an IT service and associated business processes. Careful distinction needs to be made between the role of Event Management and Incident Management, as only events that indicate exception to normal service operation and are determined by the Event Correlation engine to be significant are escalated to Incident Management. This means that incident records may be generated as a result of:

- End users calling the Service Desk to notify of a disruption to their normal use of IT services
- Events representing an exception that are resolved using automated means with an associated incident record also being generated for informational purposes
- An IT staff member noticing that a component of the IT infrastructure is behaving abnormally, despite no current impact on the end user community
- An end user logging an incident using self help means, which is then resolved by IT operations staff
- An external supplier observing that a portion of the IT infrastructure under their control is experiencing issues and logs an incident ticket via email

While the process of Request Fulfillment does typically operate in a similar fashion to Incident Management, a service request does not involve any (potential) disruption to an IT service.

Incident Models

INCIDENT MODELS PROVIDE A PRE-DEFINED set of steps and procedures that should be used to manage previously seen and documented incidents. They are used to help provide efficient resolution to the most frequently occurring or specialized incidents. Incident Models should define:

- The steps that should be taken to handle the incident
- The chronological order these steps should be taken in, with any dependencies or co-processing defined
- Responsibilities—who should do what
- Timescales and thresholds for completion of actions

- Escalation procedures—who should be contacted and when
- Any necessary evidence-preservation activities

Any service management tools that are used for Event and Incident Management should be utilized with the defined incident models that can automate the handling, management, and escalation of the process.

Specialized incidents include those that need routing to particular groups or ITIL® processes. An example of this is for capacity related incidents, in which the model would define what impact reduction measures could be performed before routing the incident to Capacity Management.

Major incidents

FOR THOSE INCIDENTS THAT RESULT in significant or organization-wide business impact, planning needs to consider how separate procedures should be used with shorter timescales and greater urgency to provide appropriate response and resolution. The first requirement is to define what constitutes a major incident for the organization and customers, with reference to the incident prioritization mechanisms that are used.

The key role of separate major incident procedures is to establish a fast and coordinated response that can manage and resolve the issues at hand. This may require the establishment of a team with the immediate focus of resolving the incident and reducing the associated business impact. The Service Desk maintains responsibility throughout the process so that users are kept fully informed of the incident status and progress for resolution.

Problem Management will typically be involved when major incidents occur, though the focus is not the resolution of the incident. Instead Problem Management seeks to identify the root cause of the incident, how this can be removed, and if there are any other areas of the infrastructure where this could occur (e.g., replicated infrastructure across multiple locations).

Incident Status Tracking

INCIDENTS SHOULD BE TRACKED THROUGHOUT their lifecycle to support proper handling and reporting on the status of incidents. Within the Incident Management system, status codes may be linked to incidents to indicate where they are in relation to the lifecycle. Examples of these might include:

- **Open:** An incident has been recognized but not yet assigned to a support resource for resolution
- **In progress:** The incident is in the process of being investigated and resolved
- **Resolved:** A resolution has been put in place for the incident but normal state service operation has not yet been validated by the business or end user
- **Closed:** The user or business has agreed that the incident has been resolved and that normal state operations have been restored

Activities

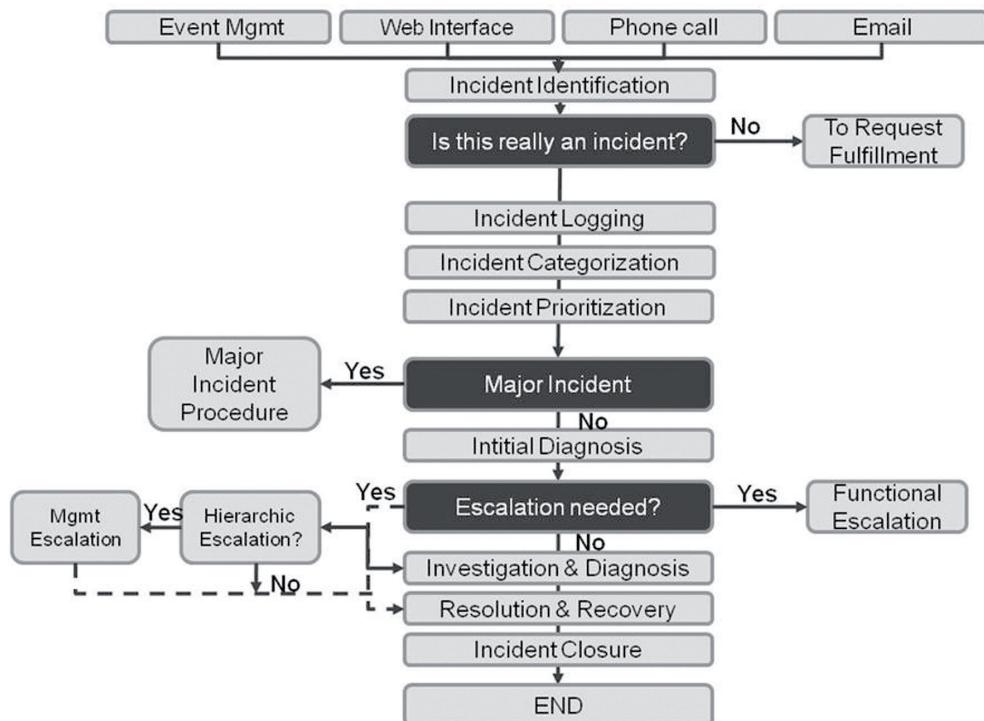


Figure 7.M—Typical Activities for Incident Management

© Crown Copyright 2011 Reproduced under license from OGC

Overview of steps

1. Incident identification
2. Incident logging
3. Incident categorization
4. Incident prioritization
5. Initial diagnosis
6. Incident escalation
7. Investigation and diagnosis
8. Resolution and recovery
9. Incident closure

1. Incident identification

The implementation of Incident Management should consider the range of sources where incidents can be identified. These typically include:

- Customers and end users
- External customers (of the business)
- IT staff members
- Automated mechanisms, including those governed by Event Management
- External suppliers

2. Incident logging

All incidents, regardless of source, must be recorded with a unique reference number and be date/time stamped. While this can be easily managed for automated mechanisms, positive behaviors need to be developed for IT staff and end users to ensure the consistent recording of identified incidents. It may also be necessary to record more than one incident for any given call/discussion so that a historical record is kept and that time/work tracking can be performed.

3. Incident categorization

During the initial logging of the incident, a category is assigned so that the exact type of incident is recorded. This information is important to allow effective escalation, trend analysis of incidents, and future infrastructure improvements. Multi-level categorization is typically used for Incident Management, where the service management tool is populated with up to three of four levels of category details.

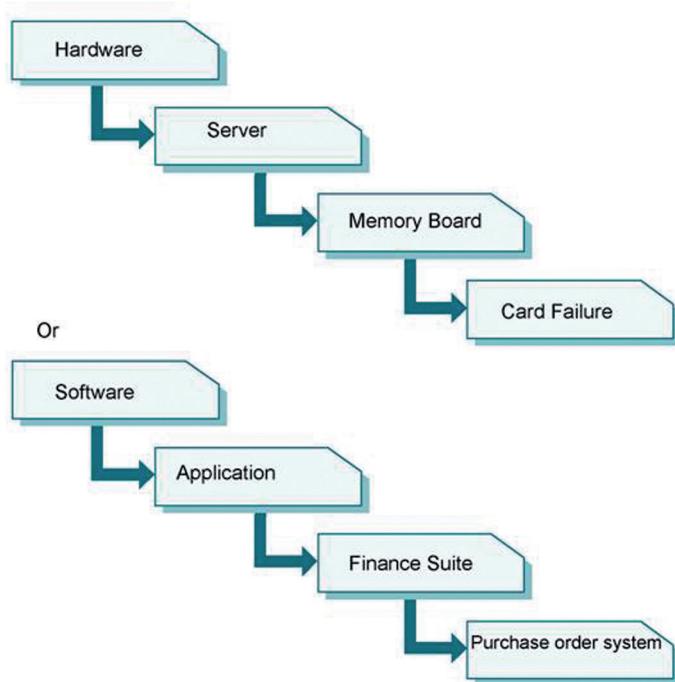


Figure 7.N—Multi-Level Incident Categorization

© Crown Copyright 2011 Reproduced under license from OGC

4. Incident prioritization

An agreed prioritization matrix should be used to determine the appropriate timescales and effort applied for response and resolution to identified incidents. The general formula by which to calculate incident priority is:

$$\text{IMPACT} + \text{URGENCY} = \text{PRIORITY}$$

- **Impact:** Degree to which the **user/business** is affected by the incident(s)
- **Urgency:** Degree to which the **resolution** of the incident can be delayed

The following factors are usually taken into account for determining the impact of an incident:

- The number of users being affected
 - (e.g., single user, multiple users, entire business unit, organization wide)
- Possible risk of injury or death
- The number of services affected
- The level of financial loss
- Effect on credibility and reputation of business
- Regulatory or legislative breaches

Urgency is calculated by assessing when the potential impact of the incident will be felt. In some cases the incident resolution can be delayed when the disruption to an IT service (e.g., payroll) has not yet affected business operations (but will if the service is not available in three days time).

		Urgency		
		High	Med	Low
Impact	High	1	2	3
	Med	2	3	4
	Low	3	4	5

Figure 7.0—Example Incident Prioritization Matrix

The prioritization matrix above would be accompanied by agreed timelines for resolution.

E.g. Priority 1 = Critical = 1 hour target resolution time

Priority 2 = High = 8 hours

Priority 3 = Medium = 24 hours

Priority 4 = Low = 48 hours

5. Initial diagnosis

For calls forwarded to the Service Desk, the staff member will use pre-defined questioning techniques to assist in the collection of useful information for the incident record. At this point, the Service Desk analyst can begin to provide some initial support by referencing known errors and simple diagnostic tools. Where possible, the incident will be resolved using these sources of information, closing the incident after verifying the resolution was successful.

For incidents that cannot be resolved at this stage and the user is still on the phone, the Service Desk analyst should inform the user of the next steps that will be

taken, give the unique incident reference number, and confirm user contact details for follow-ups.

6. Incident escalation

If the Service Desk analyst requires assistance from other groups due to an inability to resolve the incident or because of specialized circumstances (e.g., VIP user), escalation will be utilized to transfer the incident to the appropriate party or group. Rules for escalation should be defined when implementing Incident Management and agreed upon by all involved groups and stakeholders.

The two forms of escalation that are typically used are functional (horizontal) and hierarchical (vertical) escalation. Escalations can also be combined.

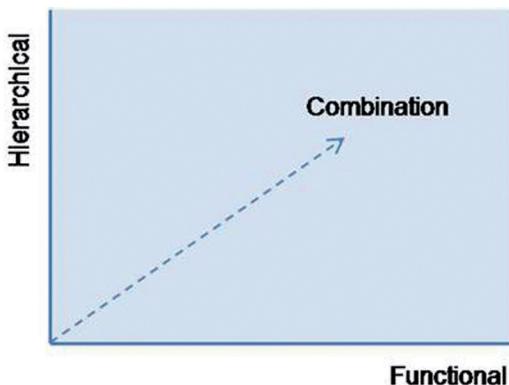


Figure 7.P—Example Incident Prioritization Matrix

Functional:

- Based on *knowledge* or *expertise*
- Also known as Horizontal Escalation, through level 1, 2, and 3 support

Hierarchical:

- For corrective actions by authorized *line management*
- Also known as Vertical Escalation
- When resolution of an incident will not be in time or satisfactory

7. Investigation and diagnosis

The incident investigation is likely to include such actions as:

- Establishing exactly what has gone wrong or what is being sought by the user
- Understanding the chronological order of events
- Confirming the full impact of the incident, including the number and range of users affected
- Identifying any events that could have triggered the incident
- Knowledge searches looking for previous occurrences by searching previous incident/problem records and/or known error databases etc.
- Seeking knowledge from system developers as to possible guidance for resolution

8. Resolution and recovery

When a potential resolution has been identified, it should be applied and tested in a controlled manner. The specific requirements for performing this will vary depending on the elements required for resolution, but could involve:

- Guiding the user to perform specific actions on their own equipment
- Specialist support groups performing specific actions on the infrastructure (such as rebooting a server)
- External suppliers performing updates on their infrastructure in order to resolve the incident
- The Service Desk or other specialist staff controlling a user's desktop remotely in order to resolve the incident

9. Incident closure

Depending on the nature of the incident (level of impact, users affected, etc.), the Service Desk may be required to call the affected users and confirm that the users are satisfied that the resolution was successful and that the incident can be closed. For other incidents, closure mechanisms may be automated and communicated via email. Closure mechanisms, whether automated or manual, should also check for the following:

- Closure categorization, with comparison to the initial categorization to ensure accurate historical tracking
- User satisfaction survey, usually be email or web-forms for an agreed percentage of random incidents

- Incident documentation, ensuring all required fields are completed satisfactorily
- Potential problem identification, assisting Problem Management in the decision of whether any preventative action is necessary to avoid this in the future

When the requirements for incident documentation are complete, the incident should be closed via agreed methods.

Roles and Responsibilities

- **Incident Manager:**
 - Drive effectiveness and efficiency of process
 - Manage incident management team
 - Ensure SLA targets for incident resolution are met
- **Skills:** Analytical, technical, business understanding, communication, calm under pressure
- **Service Desk:**
 - Log/record incidents
 - Incident classification and categorization
 - Provide initial support
 - Match to existing incident or problem records
 - Manage communication with end users
- **1st, 2nd, 3rd line support groups (including Technical and Application Management):**
 - Incident classification
 - Investigation and resolution of incidents

Inputs

EXAMPLES OF INPUTS TO THE Incident Management process may include:

- Information about Cls and their status
- Information about known errors and their workarounds
- Communication and feedback about incidents and their symptoms

- Communication and feedback about RFCs and releases that have been implemented or planned for implementation
- Communication of events that were triggered from Event Management
- Operational and service level objectives
- Customer feedback on success of incident resolution activities and overall quality of incident management activities
- Agreed criteria for prioritizing and escalating incidents

Outputs

EXAMPLES OF OUTPUTS FROM THE Incident Management process may include:

- Resolved incidents and actions taken to achieve their resolution
- Updated Incident Management records with accurate incident detail and history
- Updated classification of incidents to be used to support proactive Problem Management activities
- Raising of problem records for incidents where an underlying cause has not been identified
- Validation that incidents have not recurred for problems that have been resolved
- Feedback on incidents related to changes and releases
- Identification of CIs associated with or impacted by incidents
- Satisfaction feedback from customers who have experienced incidents
- Feedback on level and quality of monitoring technologies and Event Management activities
- Communications about incident and resolution history detail to assist with identification of overall service quality

Problem Management

Terminology

Term	Definition
escalation	(ITIL® Service Operation) An activity that obtains additional resources when these are needed to meet service level targets or customer expectations. Escalation may be needed within any IT service management process but is most commonly associated with incident management, problem management, and the management of customer complaints. There are two types of escalation: functional escalation and hierarchic escalation.
functional escalation	(ITIL® Service Operation) Transferring an incident, problem, or change to a technical team with a higher level of expertise to assist in an escalation.
hierarchic escalation	(ITIL® Service Operation) Informing or involving more senior levels of management to assist in an escalation.
impact	(ITIL® Service Operation) (ITIL® Service Transition) A measure of the effect of an incident, problem, or change on business processes. Impact is often based on how service levels will be affected. Impact and urgency are used to assign priority.
incident	(ITIL® Service Operation) An unplanned interruption to an IT service or reduction in the quality of an IT service. Failure of a configuration item that has not yet affected service is also an incident—for example, failure of one disk from a mirror set.
known error	(ITIL® Service Operation) A problem that has a documented root cause and a workaround. Known errors are created and managed throughout their lifecycle by problem management. Known errors may also be identified by development or suppliers.
known error database (KEDB)	(ITIL® Service Operation) A database containing all known error records. This database is created by problem management and used by incident and problem management. The known error database may be part of the configuration management system or may be stored elsewhere in the service knowledge management system.
known error record	(ITIL® Service Operation) A record containing the details of a known error. Each known error record documents the lifecycle of a known error, including the status, root cause, and workaround. In some implementations, a known error is documented using additional fields in a problem record.

Term	Definition
proactive problem management	(ITIL® Service Operation) Part of the problem management process. The objective of proactive problem management is to identify problems that might otherwise be missed. Proactive problem management analyzes incident records and uses data collected by other IT service management processes to identify trends or significant problems.
problem	(ITIL® Service Operation) A cause of one or more incidents. The cause is not usually known at the time a problem record is created, and the problem management process is responsible for further investigation.
problem record	(ITIL® Service Operation) A record containing the details of a problem. Each problem record documents the lifecycle of a single problem.
resolution	(ITIL® Service Operation) Action taken to repair the root cause of an incident or problem or to implement a workaround. In ISO/IEC 20000, resolution processes is the process group that includes incident and problem management.
root cause	(ITIL® Service Operation) The underlying or original cause of an incident or problem.
threat	A threat is anything that might exploit a vulnerability. Any potential cause of an incident can be considered a threat. For example, a fire is a threat that could exploit the vulnerability of flammable floor coverings. This term is commonly used in information security management and IT service continuity management but also applies to other areas, such as problem and availability management.
trend analysis	(ITIL® Continual Service Improvement) Analysis of data to identify time-related patterns. Trend analysis is used in problem management to identify common failures or fragile configuration items and in capacity management as a modeling tool to predict future behavior. It is also used as a management tool for identifying deficiencies in IT service management processes.
urgency	(ITIL® Service Design) (ITIL® Service Transition) A measure of how long it will be until an incident, problem, or change has a significant impact on the business. For example, a high-impact incident may have low urgency if the impact will not affect the business until the end of the financial year. Impact and urgency are used to assign priority.

Purpose

PROBLEM MANAGEMENT IS THE PROCESS responsible for managing the lifecycle of all problems. ITIL® defines a problem as the underlying cause of one or more incidents.

The purpose of Problem Management is to manage the lifecycle of all problems from first identification through further investigation, documentation, and eventual removal. Problem Management seeks to minimize the adverse impact of incidents and problems, which are caused by underlying errors within the IT Infrastructure, on the business and to proactively prevent recurrence of incidents related to these errors. In order to achieve this, Problem Management seeks to get to the root cause of incidents, document and communicate known errors, and initiate actions to improve or correct the situation.

- The objectives of the Problem Management process are to:
- Prevent problems and resulting incidents from happening
- Eliminate recurring incidents
- Minimize the impact of incidents that cannot be prevented

Scope

PROBLEM MANAGEMENT INCLUDES THE ACTIVITIES required to diagnose the root cause of incidents and to determine the resolution to those problems. It is also responsible for ensuring that the resolution is implemented through the appropriate control procedures, especially Change Management and Release and Deployment Management.

Problem Management will also maintain information about problems and the appropriate workarounds and resolutions so that the organization is able to reduce the number and impact of incidents over time. In this respect, Problem Management has a strong interface with Knowledge Management, and tools, such as the KEDB, will be used for both.

Although Incident and Problem Management are separate processes, they are closely related and will typically use the same tools and may use similar categorization, impact, and priority coding systems. This will ensure effective communication when dealing with related incidents and problems.

The Problem Management process has both reactive and proactive aspects:

- Reactive Problem Management is concerned with solving problems in response to one or more incidents
- Proactive Problem Management is concerned with identifying and solving problems and known errors before further incidents related to them can occur again
- While reactive Problem Management activities are performed in reaction to specific incident situations, proactive Problem Management activities take place as ongoing activities targeted to improve the overall availability and end user satisfaction with IT services. Examples of proactive Problem Management activities might include conducting periodic scheduled reviews of incident records to find patterns and trends in reported symptoms that may indicate the presence of underlying errors in the infrastructure.
- Conducting major incident reviews where review of 'How can we prevent the recurrence?' can provide identification of an underlying cause or error
- Conducting periodic scheduled reviews of operational logs and maintenance records identifying patterns and trends of activities that may indicate that an underlying problem might exist
- Conducting periodic scheduled reviews of event logs targeting patterns and trends of warning and exception events that may indicate the presence of an underlying problem
- Conducting brainstorming sessions to identify trends that could indicate the existence of underlying problems
- Using check sheets to proactively collect data on service or operational quality issues that may help to detect underlying problems

Reactive and proactive Problem Management activities are generally conducted within the scope of Service Operation. A close relationship exists between proactive Problem Management activities and CSI lifecycle activities that directly support identifying and implementing service improvements. Proactive Problem Management supports these activities through trending analysis and the targeting of preventive action. Identified problems from these activities will be input into the CSI register used to record and manage improvement opportunities.

** Initiated in Service Operation but generally driven as part of Continual Service Improvement.

Remember the weeding analogy used for Incident Management? Problem Management seeks to identify and remove the root cause of incidents in the IT Infrastructure.

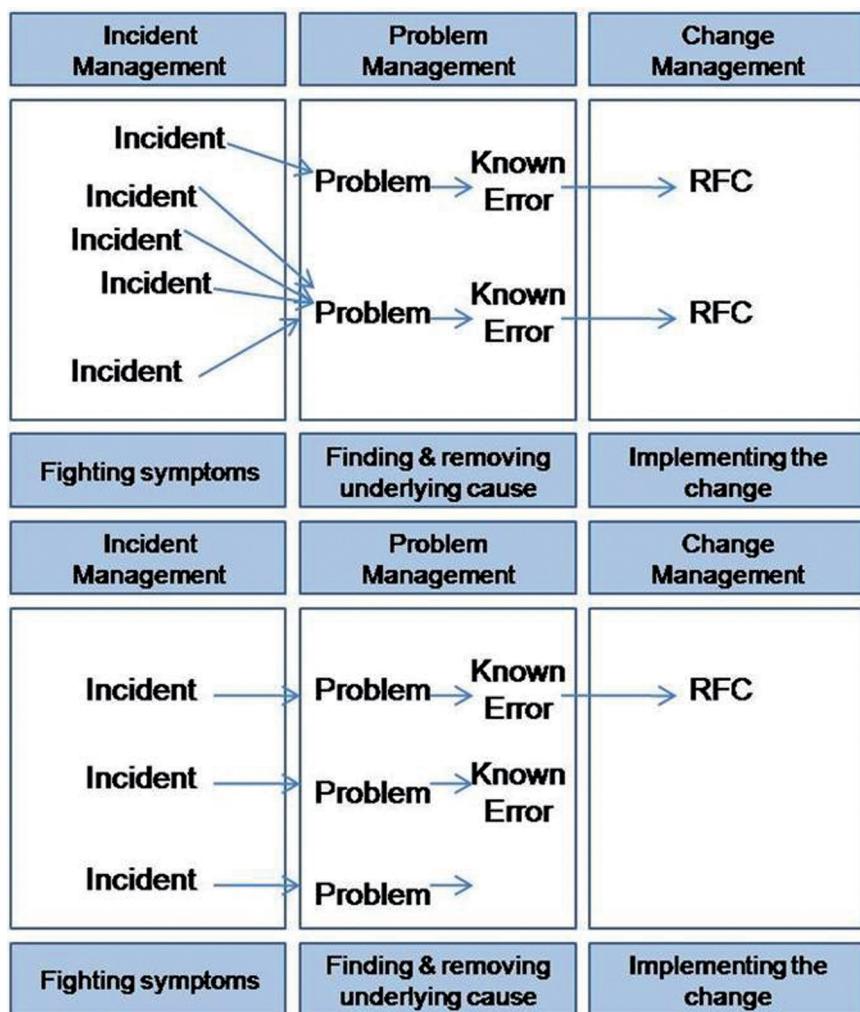


Figure 7.0—Relationships Between Incidents, Problems and Known Errors

As shown above, problems are identified and corrected in multiple ways. For most organizations, the primary benefit of Problem Management is demonstrated in the many-to-one relationship between incidents and problems. This enables an IT service provider to resolve many incidents in an efficient manner by correcting the underlying

root cause. Change Management is still required so that the actions being performed to correct and remove the error are done so in a controlled and efficient manner.

Why do some Problems not get diagnosed?

- Because the root cause is not always found

Why do some Known Errors not get fixed?

- Because we may decide that the costs exceed the benefits of fixing the error
- Because it may be fixed in an upcoming patch from development teams or suppliers

Reactive and Proactive Problem Management Activities

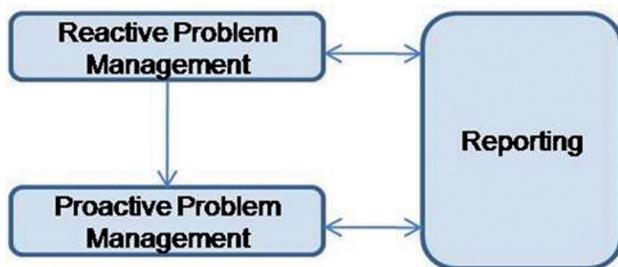


Figure 7.R—Reactive and Proactive Problem Management Activities

BOTH REACTIVE AND PROACTIVE PROBLEM Management activities seek to raise problems, manage them through the Problem Management process, find the underlying causes of the incidents they are associated with, and prevent future recurrences of those incidents. The difference between reactive and proactive Problem Management lies in how the Problem Management process is triggered:

- With reactive Problem Management, process activities will typically be triggered in reaction to an incident that has taken place. Reactive Problem Management complements Incident Management activities by focusing on the underlying cause of an incident to prevent its recurrence and identifying workarounds when necessary.
- With proactive Problem Management, process activities are triggered by activities seeking to improve services. One example might be trend

analysis activities to find common underlying causes of historical incidents that took place to prevent their recurrence. Proactive Problem Management complements CSI activities by helping to identify workarounds and improvement actions that can improve the quality of a service.

By redirecting the efforts of an organization from reacting to large numbers of incidents to preventing incidents, an organization provides a better service to its customers and makes more effective use of the available resources within the IT support organization.

Problem Models

Many problems will be unique and will require handling in an individual way, but it is conceivable that some incidents may recur because of dormant or underlying problems (for example, where the cost of a permanent resolution will be high and a decision has been taken not to go ahead with an expensive solution but to 'live with' the problem).

As well as creating a known error record in the KEDB to ensure quicker diagnosis, the creation of a Problem Model for handling such problems in the future may be helpful. This is very similar in concept to the idea of incident or request models described in previous chapters, but applied to problems.

Incidents versus problems

An incident is an unplanned interruption to an IT service or reduction in the quality of an IT service. A problem presents a different view of an incident by understanding its underlying cause, which may also be the cause of other incidents. Incidents do not become problems. While Incident Management activities are focused on restoring services to normal state operations, Problem Management activities are focused on finding ways to prevent incidents from happening in the first place. It is quite common to have incidents that are also problems.

The rules for invoking Problem Management during an incident can vary and are at the discretion of individual organizations. Some general situations where it may be desired to invoke Problem Management during an incident might include situations where:

- Incident Management cannot match an incident to existing problems and known errors
- Trend analysis of logged incidents reveals that an underlying problem might exist
- A major incident has occurred where Problem Management activities need to be undertaken to identify the root cause
- Other IT functions identify that a problem condition exists
- The Service Desk may have resolved an incident but has not determined a definitive cause and suspects that it is likely to recur
- Analysis of an incident by a support group, which reveals that an underlying problem exists or is likely to exist
- A notification from a supplier that a problem exists that has to be resolved

Reactive Problem Management

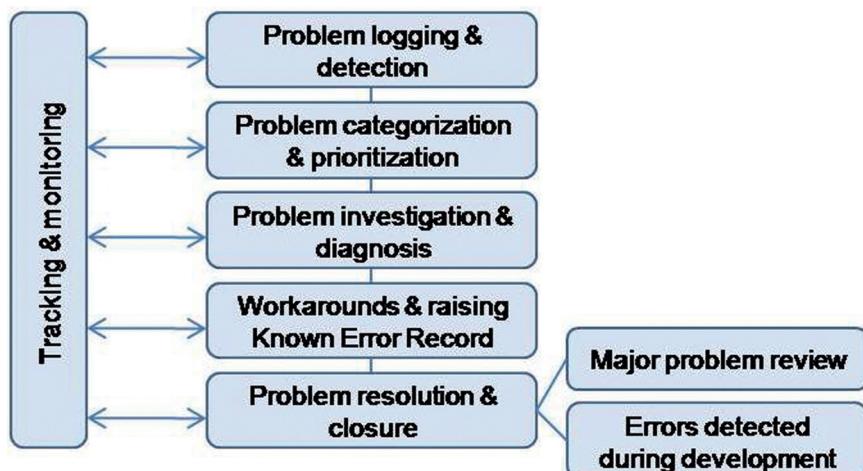


Figure 7.S—The Activities of Reactive Problem Management

THE ACTIVITIES OF REACTIVE PROBLEM Management are similar to those of Incident Management for the logging, categorization, and classification for problems. The subsequent activities are different as this is where the actual root-cause analysis is performed and the Known Error corrected.

Overview of reactive Problem Management activities:

1. Problem detection
2. Problem logging
3. Problem categorization
4. Problem investigation and diagnosis
5. Workarounds (attached to the Problem or Known Error record)
6. Raising a Known Error record
7. Problem resolution
8. Problem closure
9. Major problem reviews

Major problem review:

After every major problem, while memories are still fresh, a review should be conducted to learn any lessons for the future. Specifically, the review should examine:

- Those things that were done correctly
- Those things that were done wrong
- What could be done better in the future?
- How to prevent recurrence
- Whether there has been any third-party responsibility and whether follow-up actions are needed

Such reviews can be used as part of training and awareness activities for staff—any lessons learned should be documented in appropriate procedures, working instructions, diagnostic scripts, or Known Error Records.

Proactive Problem Management

THE TWO MAIN ACTIVITIES OF proactive Problem Management are:

Trend analysis

- Review reports from other processes (e.g., trends in incidents, availability levels, relationships with changes and releases)
- Identify recurring problems or training opportunities for IT staff, customers, and end users.

Targeting preventative action

- Perform a cost-benefit analysis of all costs associated with prevention
- Target specific areas taking up the most support attention
- Coordinate preventative action with Availability and Capacity Management, focusing on vulnerable areas of the infrastructure (e.g., single points of failure, components reaching full capacity/utilization)

Inputs

EXAMPLES OF INPUTS TO THE Problem Management process may include:

- Incident records for incidents that have triggered Problem Management activities
- Incident reports and histories that will be used to support proactive problem trending
- Information about CLs and their status
- Communication and feedback about incidents and their symptoms
- Communication and feedback about RFCs and releases that have been implemented or planned for implementation
- Communication of events that were triggered from Event Management
- Operational and service level objectives
- Customer feedback on success of problem resolution activities and overall quality of Problem Management activities
- Agreed criteria for prioritizing and escalating problems
- Output from risk management and risk assessment activities

Outputs

EXAMPLES OF OUTPUTS FROM THE Problem Management process may include:

- Resolved problems and actions taken to achieve their resolution
- Updated Problem Management records with accurate problem detail and history
- RFCs to remove infrastructure errors
- Workarounds for incidents
- Known error records
- Problem Management reports
- Output and improvement recommendations from major problem review activity

Request Fulfillment

Terminology

Term	Definition
request model	(ITIL® Service Operation) A repeatable way of dealing with a particular category of service request. A request model defines specific agreed steps that will be followed for a service request of this category. Request models may be very simple with no requirement for authorization (e.g., password reset) or may be more complex with many steps that require authorization (e.g., provision of an existing IT service). See also request fulfillment.
service request	(ITIL® Service Operation) A formal request from a user for something to be provided—for example, a request for information or advice, to reset a password, or to install a workstation for a new user. Service requests are managed by the request fulfillment process, usually in conjunction with the service desk. Service requests may be linked to a request for change as part of fulfilling the request.

The term ‘service request’ is used as a generic description for many different types of demands that are placed upon the IT organization by the users. Many of these are typically requests for small changes that are low risk, frequently performed, low cost, etc. (e.g., a request to change a password, a request to install an additional software application onto a particular workstation, a request to relocate some items of desktop equipment) or may be just a request for information.

Their scale and frequent, low-risk nature means that they are better handled by a separate process, rather than being allowed to congest and obstruct the normal Incident and Change Management processes. Effective Request Fulfillment has a very important role in maintaining end user satisfaction with the services they are receiving and can directly impact how well IT is perceived throughout the business.

Purpose

REQUEST FULFILLMENT IS THE PROCESS responsible for managing the lifecycle of all service requests from the users.

The objectives of the Request Fulfillment process are to:

- Maintain user and customer satisfaction through efficient and professional handling of all service requests
- Provide a channel for users to request and receive standard services for which a predefined authorization and qualification process exists
- Provide information to users and customers about the availability of services and the procedure for obtaining them
- Source and deliver the components of requested standard services (e.g., licenses and software media)
- Assist with general information, complaints, or comments

Scope

THE PROCESS NEEDED TO FULFILL a request will vary depending upon exactly what is being requested but can usually be broken down into a set of activities that have to be performed. For each request, these activities should be documented into a request model and stored in the SKMS.

Some organizations will be comfortable with letting the service requests be handled through their Incident Management process (and tools)—with service requests being handled as a particular type of incident (using a high-level categorization system to identify those incidents that are in fact service requests). Note, however, that there is a significant difference here: an incident is usually an unplanned event, whereas a service request is usually something that can and should be planned.

Therefore, in an organization where large numbers of service requests have to be handled and where the actions to be taken to fulfill those requests are very varied or specialized, it may be appropriate to handle service requests as a completely separate work stream and to record and manage them as a separate record type. This is essential if reporting is desired that more accurately separates incidents from requests.

This may be particularly appropriate if the organization has chosen to widen the scope of the Service Desk to expand upon just IT-related issues and use the desk as a focal point for other types of service requests, for example, a request to service a

photocopier or even going so far as to include, for example, building management issues, such as a need to replace a light fitting or repair a leak in the plumbing.

Note that ultimately it will be up to each organization to decide and document which service requests it will handle through the request fulfillment process and which will have to go through other processes.

Request Models

As many service requests are frequently recurring, predefined Request Models should be defined that document:

- What activities are required to fulfill the request
- The roles and responsibilities involved
- Target timescales and escalation paths
- Other policies or requirements that apply

Similar to Change Models, this will enable the IT department (and the Service Desk in particular) to have a clear definition of the appropriate types of service requests and repeatable actions describing how requests should be fulfilled.

Activities

1. Menu selection

Where practical, some mechanism of self help should be utilized so that users can generate service requests using technology that interfaces with existing service management tools. This might be via a website that offers users a menu-driven interface where they can select common services and provide input details. In some instances, the fulfillment of the service request can be entirely automated using workflow, ERP, software deployment, and other tools. For others, manual activities will be required to fulfill the request using resources from the IT department, suppliers, or other parties involved in the provision of IT services.

2. Financial Approval

While the service request may already have approval from Change Management, there may be some form of financial approval that is required when there are financial implications (usually those above a defined dollar amount). It may be possible to agree upon fixed prices for standard requests, otherwise the cost must be estimated and submitted to the user/customer for financial approval (who may in turn require their own line management/financial approval).

3. Other Approval

Where there may be compliance and regulatory implications for the service request, wider business approval may be needed. These approval mechanisms should be built into the request models as appropriate. Change Management should establish that there are mechanisms in place to check for and safeguard these conditions in order for the standard change to be qualified for preapproval.

4. Fulfillment

The tasks required for Fulfillment will vary depending on the characteristics of the service request at hand. Some requests can be fulfilled using only automated mechanisms. Others may be fulfilled by the Service Desk at the first-line or escalated, where necessary, to internal or external specialist groups. To ensure compatibility, Request Fulfillment should be interfaced with existing procurement and supplier processes; however, the Service Desk should maintain control and visibility for all requests regardless of where it is fulfilled.

5. Closure

When the Service Request has been fulfilled, it should be referred back to the Service Desk to initiate closure. This should include some verification that the request has been satisfied using either confirmation with the end user or other automated means.

Inputs

EXAMPLES OF INPUTS TO THE Request Fulfillment process can include:

- Work requests
- Authorization forms
- Service requests
- RFCs
- Requests from various sources, such as phone calls, web interfaces, or email
- Request for information

Outputs

EXAMPLES OF OUTPUTS FROM THE Request Fulfillment process may include:

- Authorized/rejected service requests
- Request fulfillment status reports
- Fulfilled service requests
- Incidents (rerouted)
- RFCs/standard changes
- Asset/CI updates
- Updated request records
- Closed service requests
- Cancelled service requests

Access Management

ACCESS MANAGEMENT IS THE PROCESS of granting authorized users the right to use a service, while preventing access to non-authorized users. It has also been referred to as rights management or identity management in different organizations.

Terminology

Term	Definition
rights	(ITIL® Service Operation) Entitlements or permissions granted to a user or role—for example, the right to modify particular data or to authorize a change.

Purpose

THE PURPOSE OF **ACCESS MANAGEMENT** is to provide the right for users to be able to use a service or group of services. It is, therefore, the execution of policies and actions defined in Information Security Management.

The objectives of the Access Management process are to:

- Manage access to services based on policies and actions defined in Information Security Management (see ITIL® Service Design)
- Efficiently respond to requests for granting access to services, changing access rights, or restricting access, ensuring that the rights being provided or changed are properly granted
- Oversee access to services and ensure rights being provided are not improperly used

Scope

ACCESS MANAGEMENT IS EFFECTIVELY THE execution of the policies in Information Security Management, in that it enables the organization to manage the confidentiality, availability and integrity of the organization's data and intellectual property.

Access Management ensures that users are given the right to use a service, but it does not ensure that this access is available at all agreed times—this is provided by Availability Management.

Access Management is a process that is executed by all Technical and Application Management functions and is usually not a separate function. However, there is likely to be a single control point of coordination, usually in IT Operations Management or on the Service Desk.

Access Management can be initiated by a service request.

Relationship with Other Processes

As described above, Access Management is often centrally coordinated by the Service Desk (being the single point of contact with the end user community) but can involve the Technical and Application Management functions. Where access is controlled by external suppliers, interfaces need to be developed to coordinate requests for/ modifications to access levels.

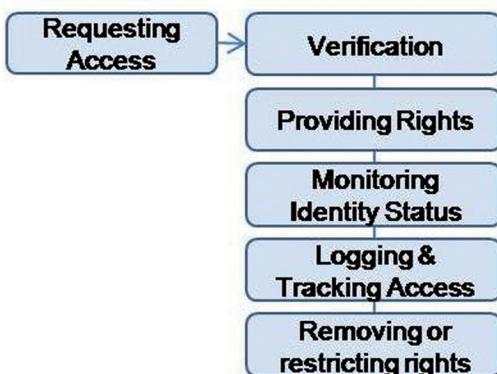


Figure 7.T—Access Management Activities

FIGURE 7.T DEMONSTRATES THE LIFECYCLE for managing access to services, information, and facilities. In many implementations, these activities relate to the lifecycle of a user as they join the organization, change roles (possibly many times), and finally leave the organization. There should be integration with existing business processes for human resources so that access levels can be continually checked for accuracy against defined job roles.

Request access

Access (or restriction) can be requested using one of any number of mechanisms, including:

- A service request generated by the human resource system. This is generally done whenever a person is hired, promoted, transferred, or when they leave the company
- An RFC
- A service request submitted via the Request Fulfillment system
- By executing a pre-authorized script or option (e.g., downloading an application from a staging server as and when it is needed)

Rules for requesting access are normally documented as part of the Request Fulfillment model associated with requests for access and may also be described in the Service Catalog.

Verification

Access Management needs to verify every request for access to an IT service from two perspectives:

- That the user requesting access is who they say they are
- That they have a legitimate requirement for that service

The first perspective is usually achieved by the user providing their user name and password. Depending on the organization's security policies, the use of the user name and password are usually accepted as proof that the person is a legitimate user. However, for more sensitive services, further authentication may be required (biometric, use of an electronic access key, encryption device, database of secret questions and answers known only to the user, etc.).

The second perspective will require some independent verification, other than the user's request. For example:

- Notification from human resources that the person is a new employee and requires both a user name and access to a standard set of services
- Notification from human resources that the user has been promoted and requires access to additional resources
- Authorization from an appropriate (defined in the process) manager
- Submission of a service request (with supporting evidence) through the Service Desk
- Submission of an RFC (with supporting evidence) through Change Management, or execution of a predefined standard change
- A policy stating that the user may have access to an optional service if they need it

For new services, the change record should specify which users or groups of users will have access to the service. Access Management will then check to see that all the users are still authorized and automatically provide access as specified in the RFC.

Provide rights

Access Management does not decide who has access to which IT services. Rather, Access Management executes the policies and regulations defined during Service Strategy and Service Design. Access Management enforces decisions to restrict or provide access, rather than making the decision.

As soon as a user has been verified, Access Management will provide that user with rights to use the requested service. In most cases, this will result in a request to every team or department involved in supporting that service to take the necessary action. If possible, these tasks should be automated.

The more roles and groups that exist, the more likely that role conflict will arise. Role conflict in this context refers to a situation where two specific roles or groups, if assigned to a single user, will create issues with separation of duties or conflict of interest. Examples of this include:

- One role requires detailed access, while another role prevents that access
- Two roles allow a user to perform two tasks that should not be combined (e.g., a contractor can log their time sheet for a project and then approve all payment on work for the same project)

Role conflict can be avoided by careful creation of roles and groups, but more often they are caused by policies and decisions made outside of service operation—either by the business or by different project teams working during Service Design. In each case, the conflict must be documented and escalated to the stakeholders to resolve.

Whenever roles and groups are defined, it is possible that they could be defined too broadly or too narrowly. There will always be users who need something slightly different from the predefined roles. In these cases, it is possible to use standard roles and then add or subtract specific rights as required—similar to the concept of baselines and variants in Service Asset and Configuration Management (see *ITIL® Service Transition*). However, the decision to do this is not in the hands of individual operational staff members. Each exception should be coordinated by Access Management and approved through the originating process.

Access Management should perform a regular review of the roles and groups that it has created and ensure that they are appropriate for the services that IT delivers and supports—any obsolete or unwanted roles/groups should be removed.

Check and monitor identity status

As users work in the organization, their roles change and so do their needs to access services. Examples of changes include:

- Job changes: In this case, the user will possibly need access to different or additional services.
- Promotions or demotions: The user will probably use the same set of services but will need access to different levels of functionality or data.
- Transfers: In this situation, the user may need access to exactly the same set of services but in a different region with different working practices and different sets of data.
- Resignation or death: Access needs to be completely removed to prevent the user name being used as a security loophole.
- Retirement: In many organizations, an employee who retires may still have access to a limited set of services, including benefits systems or systems that allow them to purchase company products at a reduced rate.
- Disciplinary action: In some cases, the organization will require a temporary restriction to prevent the user from accessing some or all of the services that they would normally have access to. There should be a feature in the process and tools to do this, rather than having to delete and reinstate the user's access rights.
- Dismissals: Where an employee or contractor is dismissed or where legal action is taken against a customer (for example, for defaulting on payment for products purchased on the internet), access should be revoked immediately. In addition, Access Management, working together with Information Security Management, should take active measures to prevent and detect malicious action against the organization from that user.

Access Management should understand and document the typical user lifecycle for each type of user and use it to automate the process. Access Management tools should provide features that enable a user to be moved from one state to another or from one group to another easily and with an audit trail.

Log and track access

Access Management should not only respond to requests; it is also responsible for ensuring that the rights they have provided are being properly used.

In this respect, access monitoring and control must be included in the monitoring activities of all Technical and Application Management functions and all service operation processes.

Exceptions should be handled by Incident Management, possibly using incident models specifically designed to deal with abuse of access rights. Note that the visibility of such actions should be restricted. Making this information available to all who have access to the Incident Management system will expose vulnerabilities.

Information Security Management plays a vital role in detecting unauthorized access and comparing it with the rights that were provided by Access Management. This will require Access Management involvement in defining the parameters for use in intrusion detection tools.

Access Management may also be required to provide a record of access for specific services during forensic investigations. If a user is suspected of breaches of policy, inappropriate use of resources, or fraudulent use of data, Access Management may be required to provide evidence of dates, times, and even content of that user's access to specific services. This is normally provided by the operational staff of that service but working as part of the Access Management process.

Remove or restrict rights

Just as Access Management provides rights to use a service, it is also responsible for revoking those rights. Again, this is not a decision that it makes on its own. Rather, it will execute the decisions and policies made during Service Strategy and Design and also decisions made by managers in the organization.

Removing access is usually done in the following circumstances:

- Death
- Resignation
- Dismissal
- When the user has changed roles and no longer requires access to the service
- Transfer or travel to an area where different regional access applies

In other cases, it is not necessary to remove access but just to provide tighter restrictions. These could include reducing the level, time, or duration of access. Situations in which access should be restricted include:

- When the user has changed roles or been demoted and no longer requires the same level of access
- When the user is under investigation but still requires access to basic services, such as email. In this case, their email may be subject to additional scanning (but this would need to be handled very carefully and in full accordance with the organization's security policy)
- When a user is away from the organization on temporary assignment and will not require access to that service for some time

Inputs

EXAMPLES OF INPUTS TO Access Management may include:

- Information security policies (from Service Design)
- Operational and service level requirements for granting access to services, performing Access Management administrative activities and responding to Access Management related events
- Authorized RFCs to access rights
- Authorized requests to grant or terminate access rights

Outputs

EXAMPLES OF OUTPUTS FROM Access Management may include:

- Provision of access to IT services in accordance with information security policies
- Access Management records and history of access granted to services
- Access Management records and history where access has been denied and the reasons for the denial
- Timely communications concerning inappropriate access or abuse of services

Service Operation Summary

FROM A CUSTOMER VIEWPOINT, **SERVICE** Operation is where actual value is seen. This is because it is the execution of strategies, designs and plans, and improvements from the Service Lifecycle stages.

Key benefits delivered as a result of Service Operation are:

- Effectiveness and efficiency in IT service delivery and support
- Increased return on investment
- More productive and positive users of IT services

Other benefits can be defined as:

1. **Long term:** Over a period of time, the Service Operation processes, functions, performance, and output are evaluated. These reports will be analyzed and decisions made about whether the improvement is needed and how best to implement it through Service Design and Transition, e.g., deployment of new tools, changes to process designs, reconfiguration of the infrastructure.
2. **Short term:** Improvement of working practices within the Service Operations processes, functions, and technology itself. Generally they involve smaller improvements that do not mean changes to the fundamental nature of a process or technology, e.g., tuning, training, personnel redeployment, etc.

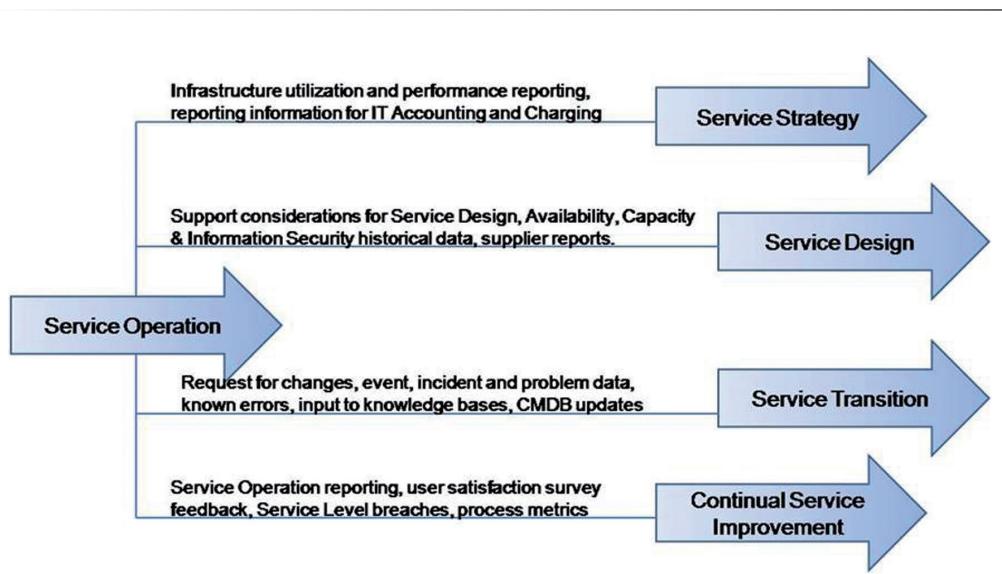


Figure 7.U—Some Outputs to Other Lifecycle Stages

Service Operation Scenario

- **Functions**

Service Desk

- Service Desk has been trained in HYPE and can support users
- Has access to known errors and workarounds to resolve incidents

Technical Management

- Designed, built, tested, and rolled HYPE out into live environment
- Supports HYPE service

Application Management

- Made modifications to HYPE application to ensure effectively interfaced with XY app
- Provided training on HYPE to users and Service Desk

IT Operations Management

- Creates backups of logs, monitors component events

- **Processes**

Event Management

- Sends alerts to IT Ops when HYPE logs backups pass/fail
- Monitors thresholds for triggers on bandwidth (set up in Availability Management)

Request Fulfillment Management

- Users use this process to request copy of logs

Access Management

- Password reset of HYPE account—provide authorized users access

Incident Management and Problem Management are not discussed in this example.

Service Operation Review Questions

Question 1

What is the best definition of an Incident Model?

- a) Predicting the impact of incidents on the network
- b) A type of incident that is used as a best practice model
- c) A set of pre-defined steps to be followed when dealing with a known type of incident
- d) An incident that requires a separate system

Question 2

What is the difference between a known error and a problem?

- a) The underlying cause of a known error is known. The underlying cause of a problem is not known
- b) A known error involves an error in the IT infrastructure. A problem does not involve such an error.

- c) A known error always originates from an incident. This is not always the case with a problem.
- d) With a problem, the relevant configuration items have been identified. This is not the case with a known error.

Question 3

Information is regularly exchanged between Problem Management and Change Management. What information is this?

- a) Known errors from Problem Management on the basis of which Change Management can generate Requests for Change (RFCs)
- b) RFCs resulting from known errors
- c) RFCs from the users that Problem Management passes on to Change Management
- d) RFCs from the Service Desk that Problem Management passes on to Change Management

Question 4

Incident Management has a value to the business by?

- a) Helping to control cost of fixing technology
- b) Enabling customers to resolve problems
- c) Helping to maximize business impact
- d) Helping to reduce the business impact

Question 5

Which of the following is NOT an example of a service request?

- a) A user calls the Service Desk to order a new mouse
- b) A user calls the Service Desk because they would like to change the functionality of an application
- c) A user calls the Service Desk to reset their password
- d) A user logs onto an internal website to download a licensed copy of software from a list of approved options

Question 6

The BEST definition of an event is?

- a) A situation where a capacity threshold has been exceeded and an agreed service level has already been impacted
- b) An occurrence that is significant for the management of the IT infrastructure or delivery of services
- c) A problem that requires immediate attention
- d) A social gathering of IT staff to celebrate the release of a service

Question 7

Technical Management is NOT responsible for?

- a) Maintenance of the local network
- b) Identifying technical skills required to manage and support the IT infrastructure
- c) Defining the service agreements for the technical infrastructure
- d) Response to the disruption to the technical infrastructure

Question 8

Which of the following is NOT an objective of Service Operation?

- a) Thorough testing to ensure that services are designed to meet business needs
- b) To deliver and support IT Services
- c) To manage the technology used to deliver services
- d) To monitor the performance of technology and processes

Question 9

Which of the following BEST describes the purpose of Event Management?

- a) The ability to detect events, analyze them, and determine the appropriate control action
- b) The ability to coordinate changes in events
- c) The ability to monitor and control projected service outages
- d) The ability to report on success of all batch processing jobs

Question 10

Which process or function is responsible for management of the Data Center facility?

- a) IT Operations Control
- b) Supplier Management
- c) Facilities Management
- d) Technical Function

Chapter 8

CONTINUAL SERVICE IMPROVEMENT



Figure 8.A—Continual Service Improvement

Processes:

- The Seven-Step Improvement process
- The main areas of focus for Continual Service Improvement (CSI) to address are:
- The overall health of ITSM as a discipline
 - Continual alignment of the portfolio of IT services with the current and future business needs
 - Maturity of the enabling IT processes for each service in a continual service lifecycle approach

Purpose

The purpose of the CSI stage of the lifecycle is to align IT services with changing business needs by identifying and implementing improvements to IT services that support business processes. These improvement activities support the lifecycle approach through Service Strategy, Service Design, Service Transition and Service Operation. CSI is always seeking ways to improve service effectiveness, process effectiveness, and cost effectiveness.

In order to identify improvement opportunities, the measurement of current performance is an important factor. Consider the following sayings about measurements and management:

- **You cannot manage what you cannot control.**
- **You cannot control what you cannot measure.**

- **You cannot measure what you cannot define.**

If services and processes are not implemented, managed, and supported using clearly defined goals, objectives, and relevant measurements that lead to actionable improvements, the business will suffer. Depending upon the criticality of a specific IT service to the business, the organization could lose productive hours, experience higher costs, suffer loss of reputation, or perhaps even risk business failure. Ultimately it could also lead to loss of customer business. That is why it is critically important to understand what to measure, why it is being measured, and what the successful outcome should be.

The objectives of CSI are to:

- Review, analyze, prioritize, and make recommendations on improvement opportunities in each lifecycle stage: Service Strategy, Service Design, Service Transition, Service Operation and CSI itself
- Review and analyze service level achievement
- Identify and implement specific activities to improve IT service quality and improve the efficiency and effectiveness of the enabling processes
- Improve cost effectiveness of delivering IT services without sacrificing customer satisfaction
- Ensure applicable quality management methods are used to support continual improvement activities
- Ensure that processes have clearly defined objectives and measurements that lead to actionable improvements
- Understand what to measure, why it is being measured, and what the successful outcome should be

Scope

ITIL® CONTINUAL SERVICE IMPROVEMENT PROVIDES guidance in four main areas:

- The overall health of ITSM as a discipline
- The continual alignment of the Service Portfolio with the current and future business needs
- The maturity and capability of the organization, management, processes, and people utilized by the services

- Continual improvement of all aspects of the IT service and the service assets that support them

To implement CSI successfully, it is important to understand the different activities that need to be applied. The following activities support CSI:

- Reviewing management information and trends to ensure that services are meeting agreed service levels
- Reviewing management information and trends to ensure that the output of the enabling processes are achieving the desired results
- Periodically conducting maturity assessments against the process activities and associated roles to demonstrate areas of improvement or, conversely, areas of concern
- Periodically conducting internal audits verifying employee and process compliance
- Reviewing existing deliverables for appropriateness
- Periodically proposing recommendations for improvement opportunities
- Periodically conducting customer satisfaction surveys
- Reviewing business trends and changed priorities and keeping abreast of business projections
- Conducting external and internal service reviews to identify CSI opportunities
- Measuring and identifying the value created by CSI improvements

These activities do not happen automatically. They must be owned by individuals within the service provider organization who are empowered to make things happen. They must also be planned and scheduled on an ongoing basis. By default, improvement becomes a process within ITSM with defined activities, inputs, outputs, roles, and reporting levels. CSI must ensure that ITSM processes are developed and deployed in support of an end-to-end service management approach to business customers. It is essential to develop an ongoing continual improvement strategy for each of the processes as well as for the services that they support.

The deliverables of CSI must be reviewed on an ongoing basis to verify completeness, functionality, and feasibility and to ensure that they remain relevant and do not become stale and unusable. It is also important to ensure that monitoring of quality indicators and metrics will identify areas for process improvement.

Since any improvement initiative will more than likely necessitate changes, specific improvements will need to follow the defined Change Management process.

Value to the Business

SELECTING AND ADOPTING THE BEST practice as recommended in this publication will assist organizations in delivering significant benefits. It will help readers to set up CSI, and the process that supports it, and to make effective use of the process to facilitate the effective improvement of service quality.

Adopting and implementing standard and consistent approaches for CSI will:

- Lead to a gradual and continual improvement in service quality, where justified
- Ensure that IT services remain continuously aligned to business requirements
- Result in gradual improvements in cost effectiveness through a reduction in costs and/or the capability to handle more work at the same cost
- Use monitoring and reporting to identify opportunities for improvement in all lifecycle stages and in all processes
- Identify opportunities for improvements in organizational structures, resourcing capabilities, partners, technology, staff skills and training, and communications

Major Concepts

The Continual Service Improvement Approach

THE CSI APPROACH PROVIDES THE basis by which improvements to IT Service Management processes can be made. They are questions to ask in order to ensure all the required elements are identified to achieve the improvements desired.

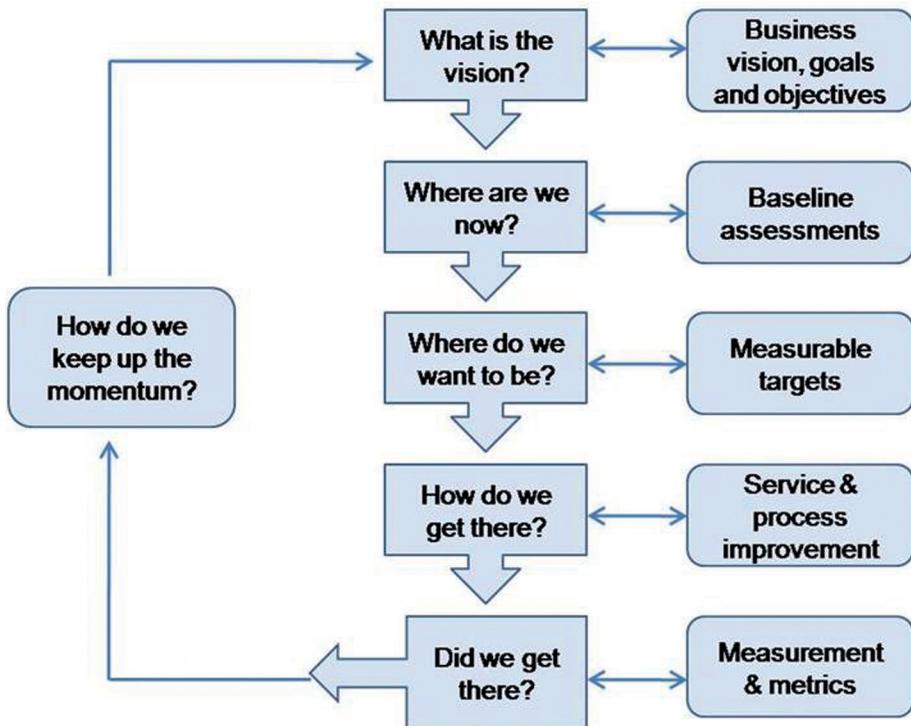


Figure 8.B—Continual Service Improvement Approach

© Crown Copyright 2011 Reproduced under license from OGC

THE CONTINUAL SERVICE IMPROVEMENT APPROACH summarizes the constant cycle for improvement. While there may be a focus on a particular lifecycle stage, the questions require close interactions with all the other ITIL® processes in order to achieve Continual Service Improvement.

Example improvement initiative for Service Operation:

- **What is the Vision?** Defining what wants to be achieved by improving Service Operation. Is the focus on service quality, compliance, security, costs, or customer satisfaction? What is the broad approach that we should take?
- **Where are we now?** Baselines taken by performing maturity assessments and by identifying what practices are currently being used (including informal and ad-hoc processes). What information can be provided by the Service Portfolio regarding strengths, weaknesses, risks, and priorities of the service provider?
- **Where do we want to be?** Defining key goals and objectives that wish to be achieved by the formalization of Service Operation processes, including both short-term and long-term targets.
- **How do we get there?** Perform a gap analysis between the current practices and defined targets to begin developing plans to overcome these gaps. Typically, the process owners and Service Operation manager will oversee the design/improvement of the processes, making sure they are fit for purpose and interface as needed with other service management processes.
- **Did we get there?** At agreed time schedules, checks should be made as to how the improvement initiatives have progressed. Which objectives have been achieved? Which haven't? What went well and what went wrong?
- **How do we keep the momentum going?** Now that the targets and objectives have been met, what is the next course of improvements that can be made? This should feed back into re-examining the vision and following the CSI approach steps again.

Since Continual Service Improvement involves ongoing change, it is important to develop an effective communication strategy to support CSI activities and ensure people remain appropriately informed. This communication must include aspects of:

- What the service implications are
- What the impact on personnel will be
- Approach/process used to reach the objective

If this communication does not exist, staff will fill the gaps with their own perceptions. Proper reporting should assist in addressing any misconceptions about improvements.

To aid in understanding the differences in perception between the service provider and the customer, a Service Gap Model can be used. This identifies the most obvious potential gaps in the Service Lifecycle from both a business and IT perspective.

SLM will produce Service Improvement Plans (SIPs) to meet the identified gaps.

Relationships within the Service Lifecycle:

- **What is the Vision?** Service Strategy, Service Portfolio
- **Where are we now?** Baselines taken using Service Portfolios, Service Level Management, and Financial Management for IT, etc.
- **Where do we want to be?** Service Portfolio, Service Measurement and Reporting
- **How do we get there?** CSI and all ITIL® processes
- **Did we get there?** Service Measurement and Reporting
- **How do we keep the momentum going?** Continual Service Improvement

The Deming Cycle

IN THE 1950s, W. EDWARDS Deming proposed that business processes should be analyzed and measured to identify sources of variations that cause products to deviate from customer requirements. He recommended that business processes be placed in a continuous feedback loop so that managers and supporting staff can identify and change the parts of the process that need improvements. As a theorist, Deming created a simplified model to illustrate this continuous process, commonly known as the PDCA cycle for Plan, Do, Check, Act:

- **Plan:** Design or revise business process components to improve results
- **Do:** Implement the plan and measure its performance
- **Check:** Assess the measurements and report the results to decision-makers
- **Act:** Decide on changes needed to improve the process

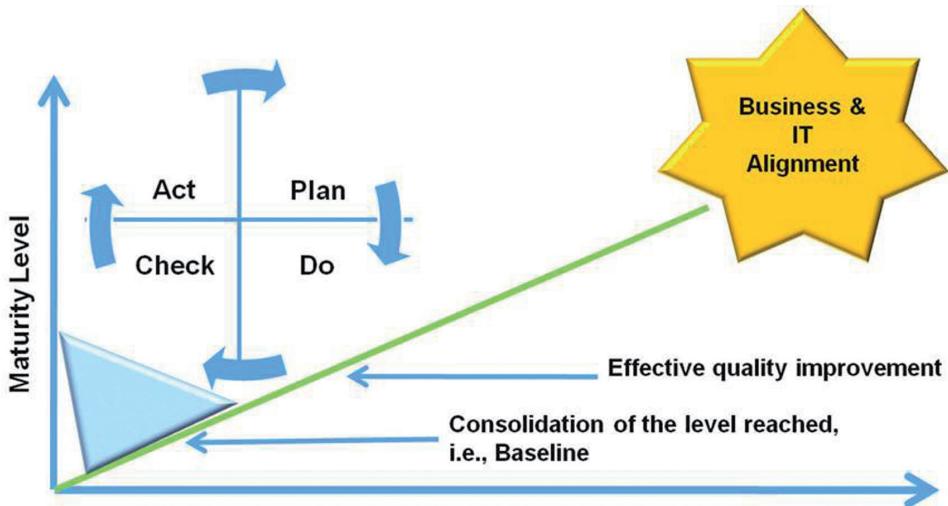


Figure 8.C—Plan-Do-Check-Act Cycle

© Crown Copyright 2011 Reproduced under license from OGC

TOO OFTEN ORGANIZATIONS ARE LOOKING for a big-bang approach to improvements. It is important to understand that a succession or series of small, planned increments of improvements will not stress the infrastructure as much and they will eventually amount to a large amount of improvement over time.

So in relation to Continual Service Improvement, the PDCA model can be applied with the following steps.

1. Plan—scope, establishing goals, objectives and requirements, interfaces, process activities, framework of roles and responsibilities, appropriate tools, methods and techniques for measuring, assessing, analyzing, and reporting
2. Do (implement)—funding and budgets, documenting and allocation roles and responsibilities, documentation and maintaining CSI policies, plans and procedures, communication and training, ensuring monitoring, analysis and trend evaluating, and reporting tools are in place, integration with the other lifecycle stages
3. Check (monitor, measure, review)—reporting against plans, documentation review, conducting process assessments and audits. The key here is identifying and recommending CSI process improvement opportunities.
4. Act—implementing actual CSI enhancements (e.g., updating CSI policies, procedures, roles, and responsibilities)

CSI Register

IT IS LIKELY THAT SEVERAL initiatives or possibilities for improvement are identified. It is recommended that a CSI register is kept to record all the improvement opportunities and that each one should be categorized into small, medium, or large undertakings. Additionally, they should be categorized into initiatives that can be achieved quickly or in the medium term or longer term. Each improvement initiative should also show the benefits that will be achieved by its implementation. With this information, a clear prioritized list can be produced. One failing that has been observed is that when something has been identified as a lower priority it never makes its way higher up the list for a further consideration, so automated raising of priorities over time may be a useful addition to the register.

The CSI register contains important information for the overall service provider and should be held and regarded as part of the Service Knowledge Management System (SKMS).

The CSI register will introduce a structure and visibility to CSI, ensuring that all initiatives are captured and recorded and benefits realized. Additionally, the benefits will be measured to show that they have given the desired results. In forecasting the benefits of each proposed improvement, we should also try to quantify the benefit in terms of aspirational key performance indicator (KPI) metrics. This will assist in prioritizing those changes that deliver the most significant incremental benefit to the business.

The CSI register provides a coordinated, consistent view of the potentially many improvement activities. It is important to define the interface from the CSI register of initiatives with strategic initiatives and with processes such as Problem Management, Capacity Management, and Change Management. In particular, the service review meeting is likely to result in a number of requirements for improvement.

The CSI manager should have accountability and responsibility for the production and maintenance of the CSI register.

IT Governance

GOVERNANCE RELATES TO DECISIONS THAT define expectations, grant power, or verify performance. It consists either of a separate process or of a specific part of management or leadership processes. In the case of a business or of a non-profit organization, governance relates to consistent management, cohesive policies, processes, and

decision-rights for a given area of responsibility. For example, managing at a corporate level might involve evolving policies on privacy, on internal investment, and on the use of data.

There are 3 main areas of governance:

- **Enterprise governance:** describes a framework that covers both corporate governance and the business management aspects of the organization. This achieves good corporate governance that is linked strategically with performance metrics and enables companies to focus all their energy on the key drivers that move their business forward.
- **Corporate governance:** concerned with promoting corporate fairness, transparency, and accountability. One example is the SOX act (2002) in the United States that was created in the aftermath of fraudulent behavior by corporate giants and states accountability provisions, such as criminal charges and incarceration for non-compliance.
- **IT governance:** responsibility of the board of directors and executive management. An integral part of enterprise governance and consists of the leadership, organizational structures, and processes that ensure the organization's IT sustains and extends the organization's strategies and objectives.

Service Measurement

Baselines

AN IMPORTANT BEGINNING POINT FOR highlighting improvement is to establish baselines as markers or starting points for later comparison. Baselines are also used to establish an initial data point to determine if a service or process needs to be improved. As a result, it is important that baselines are documented, recognized, and accepted throughout the organization. Baselines must be established at each level: strategic goals and objectives, tactical process maturity, and operational metrics and KPIs.

If a baseline is not initially established, the first measurement efforts will become the baseline. That is why it is essential to collect data at the outset, even if the integrity of the data is in question. It is better to have data to question than to have no data at all.

Examples

1. A Service Level Achievement Baseline can be used as a starting point to measure the effect of a Service Improvement Plan
2. A performance Baseline can be used to measure changes in performance over the lifetime of an IT service
3. A Configuration Management Baseline can be used to enable the IT infrastructure to be restored to a known configuration if a change or release fails

Why do we measure?

THERE ARE FOUR REASONS TO monitor and measure:

- **To validate:** monitoring and measuring to validate previous decisions
- **To direct:** monitoring and measuring to set the direction for activities in order to meet set targets—it is the most prevalent reason for monitoring and measuring
- **To justify:** monitoring and measuring to justify with factual evidence or proof that a course of action is required
- **To intervene:** monitoring and measuring to identify a point of intervention, including subsequent changes and corrective actions

The four basic reasons to monitor and measure lead to three key questions: Why are we monitoring and measuring?, When do we stop?, Is anyone using the data? To answer these questions, it is important to identify which of the above reasons is driving the measurement effort. Too often, we continue to measure long after the need has passed. Every time you produce a report you should ask: Do we still need this?

Types of Metrics

THERE ARE 3 TYPES OF metrics that an organization will need to collect to support CSI activities, as well as other process activities:

- **Technology metrics:** often associated with component and application-based metrics, such as performance, availability, etc. The various design architects and technical specialists are responsible for defining the technology metrics.

- **Process metrics:** captured in the form of Key Performance Indicators (KPIs) and activity metrics for the service management processes that determine the overall health of a process. Four key questions that KPIs can help to answer are centered on quality, performance, value, and compliance. CSI uses these metrics to identify improvement opportunities for each process. The various process owners are responsible for defining the metrics for the process that they are responsible for coordinating and managing.
- **Service metrics:** the results of the end-to-end service. Component metrics are used to calculate the service metrics. The service level manager(s) and service owners are responsible for defining appropriate service metrics.

Tension Metrics

ALL SERVICE PROVIDERS ARE FACED with the challenge of a balancing act between three main elements:

- Resources—people, IT infrastructure, consumables, and money
- Features—the product or service and its quality
- Time schedule—the timeframes within which various stages and the final delivery of a service or product are required to be achieved

The delivered product or service, therefore, represents a balanced trade-off between these three elements. Tension metrics can help create that balance by preventing teams from focusing on just one element. If an initiative is being driven primarily towards satisfying a business driver of on-time delivery to the exclusion of other factors, the manager will achieve this aim by flexing the resources and service features in order to meet the delivery schedule. This unbalanced focus will either lead to budget increase or lower product quality. Tension metrics help to create a balance between shared goals and delivering a product or service according to the business requirements within time and budget.

Seven-Step Improvement Process

FUNDAMENTAL TO CSI IS THE concept of measurement. CSI uses the seven-step improvement process shown in Figure 8.D.

The value of the seven-step improvement process is that, by monitoring and analyzing the delivery of services, it will ensure that the current and future business outcome requirements can be met. The seven-step improvement process enables continual assessment of the current situation against business needs and identifies opportunities to improve service provision for customers.

Terminology

Term	Definition
seven-step improvement process	(ITIL® Continual Service Improvement) The process responsible for defining and managing the steps needed to identify, define, gather, process, analyze, present, and implement improvements. The performance of the IT service provider is continually measured by this process and improvements are made to processes, IT services, and IT infrastructure in order to increase efficiency, effectiveness, and cost effectiveness. Opportunities for improvement are recorded and managed in the CSI register.

Purpose

THE PURPOSE OF THE SEVEN-STEP improvement process is to define and manage the steps needed to identify, define, gather, process, analyze, present, and implement improvements.

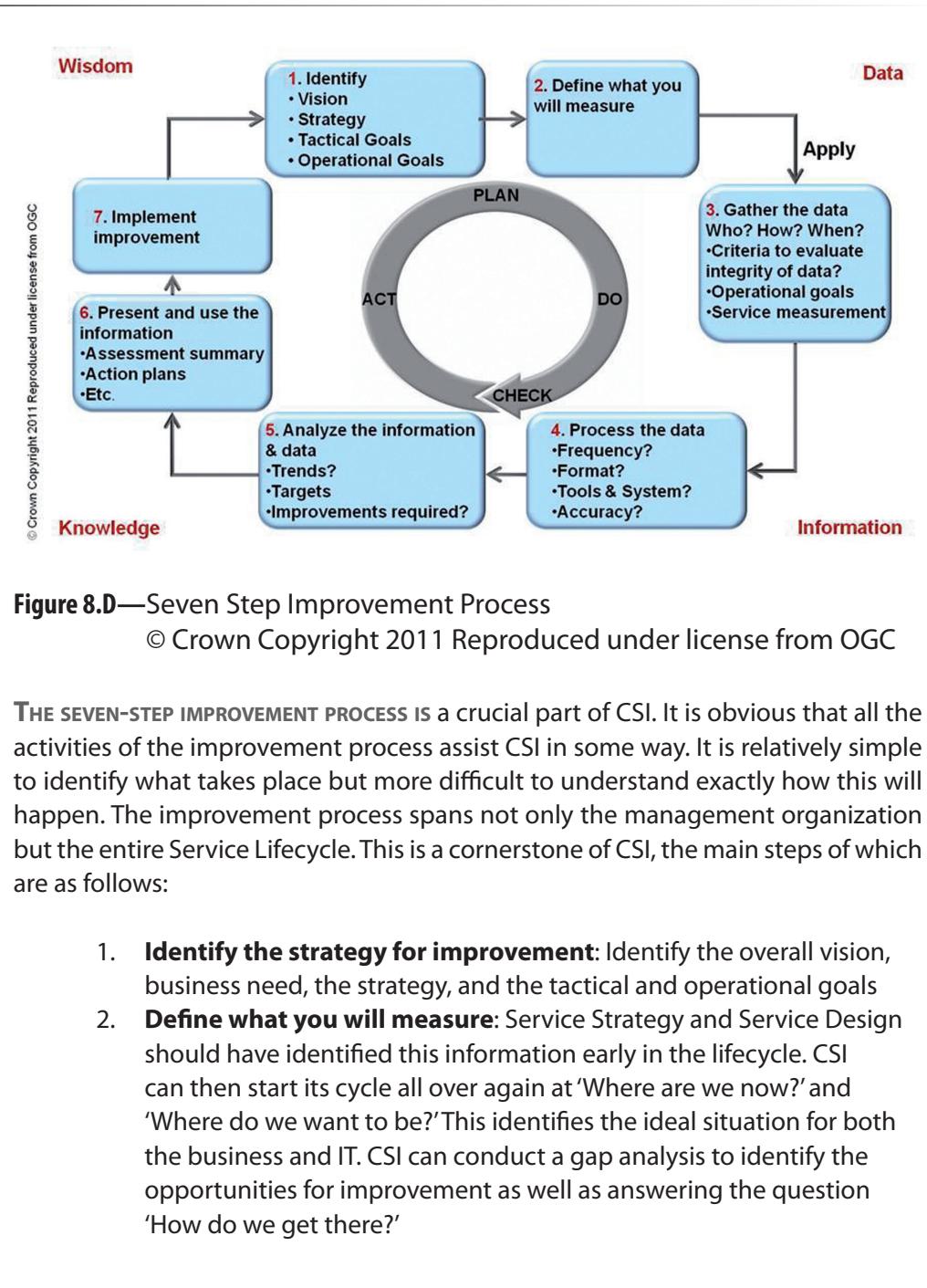
The objectives of the seven-step improvement process are to:

- Identify opportunities for improving services, processes, tools, etc.
- Reduce the cost of providing services and ensuring that IT services enable the required business outcomes to be achieved. A clear objective will be cost reduction, but this is not the only criterion. If service delivery or quality reduces as a result, the overall impact may be neutral or even negative.
- Identify what needs to be measured, analyzed, and reported to establish improvement opportunities

- Continually review service achievements to ensure they remain matched to business requirements, continually align and re-align service provision with outcome requirements
- Understand what to measure, why it is being measured, and carefully define the successful outcome
- The value of the seven-step improvement process is that by monitoring and analyzing the delivery of services, it will ensure the current and future business outcome requirements can be met. The seven-step improvement process enables continual assessment of the current situation against business needs and identifies opportunities to improve service provision for customers.

Scope

THE SEVEN-STEP IMPROVEMENT PROCESS INCLUDES analysis of the performance and capabilities of services, processes throughout the lifecycle, partners, and technology. It includes the continual alignment of the portfolio of IT services with the current and future business needs as well as the maturity of the enabling IT processes for each service. It also includes making best use of the technology that the organization has and looks to exploit new technology as it becomes available, where there is a business case for doing so. Also within the scope are the organizational structure, the capabilities of the personnel, and asking whether people are working in appropriate functions and roles and if they have the required skills.



3. **Gather the data:** In order to properly answer the question ‘Did we get there?’, data must first be gathered (usually through service operations). Data can be gathered from many different sources based on goals and objectives identified. At this point the data is raw and no conclusions are drawn.
4. **Process the data:** Here the data is processed in alignment with the critical success factors (CSFs) and KPIs specified. This means that timeframes are coordinated, unaligned data is rationalized and made consistent, and gaps in the data are identified. The simple goal of this step is to process data from multiple disparate sources to give it context that can be compared. Once we have rationalized the data we can begin analysis.
5. **Analyze the information and data:** As we bring the data more and more into context, it evolves from raw data into information where we can start to answer questions about who, what, when, where, and how, as well as trends and the impact on the business. It is the analyzing step that is most often overlooked or forgotten in the rush to present data to management.
6. **Present and use the information:** Here the answer to ‘Did we get there?’ is formatted and communicated in whatever way necessary to present to the various stakeholders an accurate picture of the results of the improvement efforts. Knowledge is presented to the business in a form and manner that reflects their needs and assists them in determining the next steps.
7. **Implement improvement:** The knowledge gained is used to optimize, improve, and correct services and processes. Issues have been identified and now solutions are implemented—wisdom is applied to the knowledge. The improvements that need to be taken to improve the service or process are communicated and explained to the organization. Following this step the organization establishes a new baseline and the cycle begins anew.

Inputs and Outputs

MONITORING TO IDENTIFY IMPROVEMENT OPPORTUNITIES is and must be an ongoing process. New incentives may trigger additional measurement activity, such as changing business requirements, poor performance with a process, or spiraling costs.

Many inputs and outputs to the process are documented within the steps discussed earlier, but examples of key inputs include:

- Service Catalog
- SLRs
- The service review meeting
- Vision and mission statements
- Corporate, divisional, and departmental goals and objectives
- Legislative requirements
- Governance requirements
- Budget cycle
- Customer satisfaction surveys
- The overall IT strategy
- Market expectations (especially in relation to competitive IT service providers)
- New technology drivers (e.g., cloud-based delivery and external hosting)
- Flexible commercial models (e.g., low capital expenditure and high operational expenditure commercial models and rental models)

Continual Service Improvement Summary

THERE IS GREAT VALUE TO the business when service improvement takes a holistic approach throughout the entire lifecycle. Continual Service Improvement enables this holistic approach to be taken.

- Some key benefits of the Continual Service Improvement stage:
- Increased growth
- Competitive Advantage
- Increased Return On Investment
- Increased Value On Investment

ROI: Return on investment—difference between the benefit (saving) achieved and the amount expended to achieve that benefit, expressed as percentage. Logically we would like to spend a little to save a lot.

VOI: Value on investment—extra value created by establishment of benefits that include non-monetary or long-term outcomes. ROI is a subcomponent of VOI.

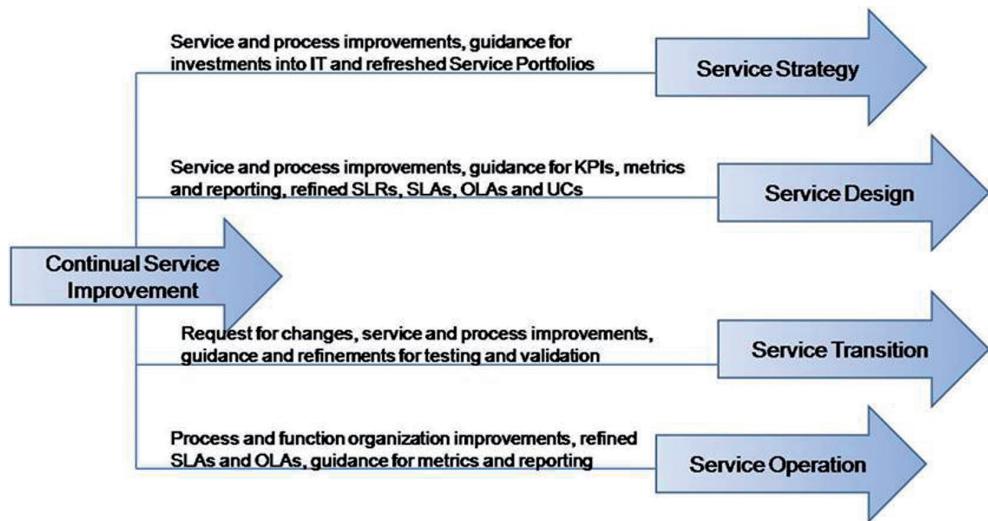


Figure 8.E—Some Outputs to Other Lifecycle Stages

Continual Service Improvement Scenario

To do this effectively, IT was necessary to take metrics and data and analyze this against targets.

The CSI improvement approach was used as a roadmap for this SIP (Service Improvement Scenario). As the business needs changed, so did the perceived value of HYPE. HYPE had become an integral part of the business communication plan. As a result, new business plans/goals were established and new targets set with an action plan for improvement.

This will identify:

- Technology improvements
- Process improvements
- Document improvements
- Training, etc.

As plans were formalized and accepted by the business, Request for Changes to technology, process, and documentation were submitted to Change Management.

And so it continues!

Continual Service Improvement Review Questions

Question 1

Why should monitoring and measuring be used when trying to improve services?

- a) To validate, justify, monitor, and improve
- b) To validate, direct, justify, and intervene
- c) To validate, check, act, and improve
- d) To validate, analyze, direct, and improve

Question 2

Which is the first activity of the Continual Service Improvement (CSI) approach?

- a) Assess the customer's requirements
- b) Understand the vision of the business
- c) Identify what can be measured
- d) Develop a plan for improvement

Question 3

The four stages of the Deming Cycle are?

- a) Plan, Assess, Check, Report
- b) Plan, Do, Check, Act
- c) Plan, Check, Revise, Improve
- d) Plan, Do, Act, Assess

Question 4

Which of the following is NOT a step in the Continual Service Improvement (CSI) approach?

- a) What is the vision?
- b) Did we get there?
- c) Who will help us get there?
- d) Where are we now?

Question 5

Which of the following provides the correct set of governance levels managed by an organization?

- a) Technology, Service, Business
- b) Financial, Legal, Security
- c) Process, Service, Technology
- d) IT, Corporate, Enterprise

ITIL® FOUNDATION EXAM TIPS

Exam Details:

- 40 questions
- The correct answer is only one of the four
- 60 minutes duration
- 26 out of 40 is a pass (65%)
- Closed book
- No notes

Practical Suggestions:

- Read the question **CAREFULLY**
- At this exam level, the obvious answer is often the correct answer (*if you have read the question carefully!*)
- Beware of being misled by the preliminary text for the question
- If you think there should be another choice that would be the right answer, then you have to choose the most right answer
- Use strategies such as "*What comes first?*" or "*What doesn't belong?*" to help with the more difficult questions
- Where there are questions that involve multiple statements (i.e., 1, 2, 3, 4), then try to eliminate combinations that are immediately incorrect (based on something you can remember) so that the question is broken into smaller and more manageable pieces.

Make sure that you prepare adequately in the lead up to your exam by reviewing your notes, reading any available material, and attempting the sample exams.

We hope this book has been of value and wish you luck in your exam and future IT Service Management career!

ANSWERS FOR REVIEW QUESTIONS

The following section provides example reasoning for each answer. This is only a guide, however, and does not cover every possible reason why an answer is correct or incorrect.

Service Strategy

ANSWERS

1c, 2a, 3b, 4c, 5b, 6a, 7d, 8b, 9b, 10d

Question 1

Which ITIL® process is responsible for developing a charging system?

- a) Availability Management
- b) Capacity Management
- c) **Financial Management for IT Services—this is an element of IT accounting and chargeback**
- d) Service Level Management

Question 2

What is the RACI model used for?

- a) **Documenting the roles and relationships of stakeholders in a process or activity—this is the primary purpose of RACI, i.e., mapping processes to functions and roles**
- b) Defining requirements for a new service or process
- c) Analyzing the business impact of an incident
- d) Creating a balanced scorecard showing the overall status of Service Management

Question 3

Which of the following identifies two Service Portfolio components within the Service Lifecycle?

- a) Catalog Service Knowledge Management System and Requirements Portfolio
- b) **Service Catalog and Service Pipeline—correct, the three areas are Pipeline, Catalog, and Retired Services**
- c) Service Knowledge Management System and Service Catalog
- d) Service Pipeline and Configuration Management System

Question 4

Which of the following is NOT one of the ITIL® core publications?

- a) Service Operation
- b) Service Transition
- c) **Service Derivation**
- d) Service Strategy

Question 5

A Service Level Package is best described as?

- a) A description of customer requirements used to negotiate a Service Level Agreement
- b) **A defined level of utility and warranty associated with a core service package—correct, a combination of utility and warranty that meets the customer's needs**
- c) A description of the value that the customer wants and for which they are willing to pay
- d) A document showing the service levels achieved during an agreed reporting period

Question 6

Setting policies and objectives is the primary concern of which of the following elements of the Service Lifecycle?

- a) **Service Strategy—see objectives of Service Strategy**
- b) Service Strategy and Continual Service Improvement
- c) Service Strategy, Service Transition, and Service Operation
- d) Service Strategy, Service Design, Service Transition, Service Operation, and Continual Service Improvement

Question 7

A service owner is responsible for which of the following?

- a) Designing and documenting a service
- b) Carrying out the service operations activities needed to support a service
- c) Producing a balanced scorecard showing the overall status of all services
- d) **Recommend improvements—correct, the service owner is responsible for continually improving their service**

Question 8

The utility of a service is best described as:

- a) Fit for design
- b) **Fit for purpose**
- c) Fit for function
- d) Fit for use

Question 9

The warranty of a service is best described as:

- a) Fit for design
- b) **Fit for use**
- c) Fit for purpose
- d) Fit for function

Question 10

The contents of a service package includes:

- a) Base Service Package, Supporting Service Package, Service Level Package
- b) Core Service Package, Supporting Process Package, Service Level Package
- c) Core Service Package, Base Service Package, Service Support Package
- d) **Core Service Package, Supporting Services Package, Service Level Package—correct, see Service Packages**

Service Design

ANSWERS

1b, 2a, 3d, 4d, 5b, 6b, 7a, 8b, 9c, 10d

Question 1

Which ITIL® process analyzes threats and dependencies to IT services as part of the decision regarding countermeasures to be implemented?

- a) Availability Management
- b) **IT Service Continuity Management**
- c) Problem Management
- d) Service Asset and Configuration Management

Question 2

What is the name of the activity within the Capacity Management process whose purpose is to predict the future capacity requirements of new and changed services?

- a) **Application Sizing**
- b) Demand Management
- c) Modeling
- d) Tuning

Question 3

In which ITIL® process are negotiations held with customers about the availability and capacity levels to be provided?

- a) Availability Management
- b) Capacity Management
- c) Financial Management for IT Services
- d) **Service Level Management—SLM is always the process that negotiates with customers about any aspect of service quality**

Question 4

Which of the following statements is false?

- a) It is impossible to maintain user and customer satisfaction during a disruption to service
- b) When reporting the availability provided for a service, the percentage (%) availability that is calculated takes into account the agreed service hours
- c) Availability of services could be improved by changes to the architecture, ITSM processes, or IT staffing levels
- d) **Reports regarding availability should include more than just uptime, downtime, and frequency of failure and reflect the actual business impact of unavailability—correct, this is called business-oriented availability reporting**

Question 5

Which of the following activities is Service Level Management responsible for?

- a) Informing users of available services
- b) **Identifying customer needs**
- c) Overseeing service release schedule
- d) Keeping accurate records of all configuration items

Question 6

Which process reviews Operational Level Agreements (OLAs) on a regular basis?

- a) Supplier Management
- b) **Service Level Management**
- c) Service Portfolio Management
- d) Contract Management

Question 7

What is another term for Uptime?

- a) **Mean Time Between Failures (MTBF)**
- b) Mean Time to Restore Service (MTRS)
- c) Mean Time Between System Incidents (MTBSI)
- d) Relationship between MTBF and MTBSI

Question 8

Which of the following is an activity of IT Service Continuity Management?

- a) Advising end users of a system failure
- b) **Documenting the recovery procedure for a critical system—correct, this is an activity of the ITSCM process**
- c) Reporting regarding availability
- d) Guaranteeing that the Configuration Items are constantly kept up - to - date

Question 9

Information security must consider the following four perspectives:

1. Organizational
2. Physical
3. Technical
4. ?

- a) Process
- b) Security

- c) **Procedural—see scope of Information Security Management**
- d) Firewalls

Question 10

The 3 types of Service Level Agreements structures are:

- a) Customer-based, Service-based, Corporate-based
- b) Corporate-level, customer-level, service-level
- c) Service-based, customer-based, user-based
- d) **Customer-based, service-based, multi-level**

Service Transition

ANSWERS

1a, 2a, 3d, 4b, 5b, 6c, 7a, 8b, 9a, 10b

Question 1

The key element of a standard change is _____?

- a) **Documentation of a pre-approved procedure for implementing the change**
- b) Low risk to the production environment—this in itself does not guarantee a standard change
- c) No requirement for service downtime—the risk of unplanned disruption may still be high
- d) It can be included in the next monthly or quarterly release—this relates to the packaging of releases, not the classification of changes

Question 2

The four phases of Release and Deployment are:

1. Release and deployment planning
2. Release build and test
3. ?

4. Review and close
 - a) **Deployment**
 - b) Change authorization
 - c) Change coordination
 - d) Release coordination

Question 3

The 4 spheres of Knowledge Management are:

- a) Data, facts, knowledge, wisdom
- b) Ideas, facts, knowledge, wisdom
- c) Data, information, facts, wisdom
- d) **Data, information, knowledge, wisdom—easier to remember as DIKW**

Question 4

Which activity in Service Asset and Configuration Management would help to ascertain whether the recorded configuration items conform to the physical environment?

- a) Control—this is the modification of CIs themselves
- b) **Verification and audit**
- c) Identification—this collects all the information to be stored for a CI
- d) Status accounting—this does not itself include validation procedures

Question 5

After a change has been implemented, an evaluation is performed. What is this evaluation called?

- a) Forward Schedule of Changes (FSC)
- b) **Post Implementation Review (PIR)**
- c) Service Improvement Program (SIP)
- d) Service Level Requirement (SLR)

Question 6

Which of the following is not a change type?

- a) Standard change
- b) Normal change
- c) **Quick change**
- d) Emergency change

Question 7

Which process is responsible for maintaining software items in the Definitive Media Library (DML)?

- a) **Release and Deployment Management—as R&D will be responsible for storing and deploying all software items in the DML**
- b) Service Asset and Configuration Management—only responsible for maintaining the records associated with the DML
- c) Service validation and testing
- d) Change Management

Question 8

Which process or function is responsible for communicating the change schedule to the users?

- a) Change Management—responsible for maintaining the change schedule but provides this to the Service Desk for communicating to users
- b) **Service Desk—should be the single point of contact for ALL user communication**
- c) Release and Deployment Management
- d) Service Level Management

Question 9

Which of the following best describes a baseline?

- a) **Used as a reference point for later comparison**
- b) The starting point of any project—only one example of a baseline
- c) The end point of any project – only one example of a baseline
- d) A rollback procedure

Question 10

The main objective of Change Management is to?

- a) Ensure that any changes are approved and recorded—not all changes are approved
- b) **Ensure that standardized methods and procedures are used for controlled handling of all changes**
- c) Ensure that any change requests are managed through the CAB—this is not true for standard changes
- d) Ensure that the CAB takes responsibility for all change implementation—CAB only coordinates implementation, the work is performed within the Release and Deployment process

Service Operation

ANSWERS

1c, 2a, 3b, 4d, 5b, 6b, 7c, 8a, 9a, 10c

Question 1

What is the best definition of an Incident Model?

- a) Predicting the impact of incidents on the network
- b) A type of incident that is used as a best practice model
- c) **A set of pre-defined steps to be followed when dealing with a known type of incident**
- d) An incident that requires a separate system

Question 2

What is the difference between a known error and a problem?

- a) **The underlying cause of a known error is known. The underlying cause of a problem is not known.**
- b) A known error involves an error in the IT infrastructure. A problem does not involve such an error.
- c) A known error always originates from an incident. This is not always the case with a problem.
- d) With a problem, the relevant configuration items have been identified. This is not the case with a known error—explanation is reversed.

Question 3

Information is regularly exchanged between Problem Management and Change Management. What information is this?

- a) Known Errors from Problem Management on the basis of which Change Management can generate Requests for Change (RFCs)—Change Management accepts the RFC, does not create it itself
- b) **RFCs resulting from Known Errors**
- c) RFCs from the users that Problem Management passes on to Change Management
- d) RFCs from the Service Desk that Problem Management passes on to Change Management

Question 4

Incident Management has a value to the business by?

- a) Helping to control cost of fixing technology
- b) Enabling customers to resolve Problems—this is problem management
- c) Helping to maximize business impact
- d) **Helping to reduce the business impact**

Question 5

Which of the following is NOT an example of a service request?

- a) A user calls the Service Desk to order a new mouse
- b) **A user calls the Service Desk because they would like to change the functionality of an application—this would be a normal change, due to the potential risk and implications of the change**
- c) A user calls the Service Desk to reset their password
- d) A user logs onto an internal website to download a licensed copy of software from a list of approved options—this is an example of a service request workflow that has been automated

Question 6

The BEST definition of an event is?

- a) A situation where a capacity threshold has been exceeded and an agreed service level has already been impacted—only one type of event (exception)
- b) **An occurrence that is significant for the management of the IT Infrastructure or delivery of services**
- c) A problem that requires immediate attention
- d) A social gathering of IT staff to celebrate the release of a service

Question 7

Technical Management is NOT responsible for?

- a) Maintenance of the local network
- b) Identifying technical skills required to manage and support the IT Infrastructure
- c) **Defining the service agreements for the technical infrastructure—this is the role of Service Level Management**
- d) Response to the disruption to the technical infrastructure

Question 8

Which of the following is NOT an objective of Service Operation?

- a) **Thorough testing to ensure that services are designed to meet business needs—this is an objective of Service Transition**
- b) To deliver and support IT Services
- c) To manage the technology used to deliver services
- d) To monitor the performance of technology and processes

Question 9

Which of the following BEST describes the purpose of Event Management?

- a) **The ability to detect events, analyze them, and determine the appropriate control action**
- b) The ability to coordinate changes in events
- c) The ability to monitor and control projected service outages—this is only one role of Event Management
- d) The ability to report on success of all batch processing jobs—this is only one role of Event Management

Question 10

Which process or function is responsible for management of the Data Center facility?

- a) IT Operations Control
- b) Supplier Management
- c) **Facilities Management**
- d) Technical Function

Continual Service Improvement

ANSWERS

1b, 2b, 3b, 4c, 5d

Question 1

Why should monitoring and measuring be used when trying to improve services?

- a) To validate, justify, monitor, and improve
- b) **To validate, direct, justify, and intervene—see Service Measurement and Reporting**
- c) To validate, check, act, and improve
- d) To validate, analyze, direct, and improve

Question 2

Which is the first activity of the Continual Service Improvement (CSI) approach?

- a) Assess the customer's requirements
- b) **Understand the vision of the business**
- c) Identify what can be measured
- d) Develop a plan for improvement

Question 3

The four stages of the Deming Cycle are?

- a) Plan, Assess, Check, Report
- b) **Plan, Do, Check, Act**
- c) Plan, Check, Revise, Improve
- d) Plan, Do, Act, Assess

Question 4

Which of the following is NOT a step in the Continual Service Improvement (CSI) approach?

- a) What is the vision?
- b) Did we get there?
- c) **Who will help us get there?**
- d) Where are we now?

Question 5

Which of the following provides the correct set of governance levels managed by an organization?

- a) Technology, Service, Business
- b) Financial, Legal, Security
- c) Process, Service, Technology
- d) **IT, Corporate, Enterprise**

Chapter 11

GLOSSARY

Term	Definition
accounting	(ITIL® Service Strategy) The process responsible for identifying the actual costs of delivering IT services, comparing these with budgeted costs, and managing variance from the budget.
activity	A set of actions designed to achieve a particular result. Activities are usually defined as part of processes or plans and are documented in procedures.
alert	(ITIL® Service Operation) A notification that a threshold has been reached, something has changed, or a failure has occurred. Alerts are often created and managed by system management tools and are managed by the event management process.
application	Software that provides functions that are required by an IT service. Each application may be part of more than one IT service. An application runs on one or more servers or clients.
application sizing	(ITIL® Service Design) The activity responsible for understanding the resource requirements needed to support a new application or a major change to an existing application. Application sizing helps to ensure that the IT service can meet its agreed service level targets for capacity and performance.
asset	(ITIL® Service Strategy) Any resource or capability. The assets of a service provider include anything that could contribute to the delivery of a service. Assets can be one of the following types: management, organization, process, knowledge, people, information, applications, infrastructure, or financial capital. See also customer asset; service asset; strategic asset.
attribute	(ITIL® Service Transition) A piece of information about a configuration item. Examples are name, location, version number, and cost. Attributes of CIs are recorded in a configuration management database (CMDB) and maintained as part of a configuration management system (CMS). See also relationship; configuration management system.

Term	Definition
availability	(ITIL® Service Design) Ability of an IT service or other configuration item to perform its agreed function when required. Availability is determined by reliability, maintainability, serviceability, performance, and security. Availability is usually calculated as a percentage. This calculation is often based on agreed service time and downtime. It is best practice to calculate availability of an IT service using measurements of the business output.
availability management information system (AMIS)	(ITIL® Service Design) A set of tools, data, and information that is used to support availability management.
baseline	<p>See also service knowledge management system.</p> <p>(ITIL® Continual Service Improvement) (ITIL® Service Transition) A snapshot that is used as a reference point. Many snapshots may be taken and recorded over time but only some will be used as baselines. For example:</p> <p>An ITSM baseline can be used as a starting point to measure the effect of a service improvement plan</p> <p>A performance baseline can be used to measure changes in performance over the lifetime of an IT service</p> <p>A configuration baseline can be used as part of a back-out plan to enable the IT infrastructure to be restored to a known configuration if a change or release fails.</p>
benchmark	<p>See also benchmark.</p> <p>(ITIL® Continual Service Improvement) (ITIL® Service Transition) A baseline that is used to compare related data sets as part of a benchmarking exercise. For example, a recent snapshot of a process can be compared to a previous baseline of that process, or a current baseline can be compared to industry data or best practice.</p>
benchmarking	<p>See also benchmarking; baseline.</p> <p>(ITIL® Continual Service Improvement) The process responsible for comparing a benchmark with related data sets, such as a more recent snapshot, industry data, or best practice. The term is also used to mean creating a series of benchmarks over time and comparing the results to measure progress or improvement. This process is not described in detail within the core ITIL® publications.</p>

Term	Definition
Best Management Practice (BMP)	<p>The Best Management Practice portfolio is owned by the Cabinet Office, part of HM Government. Formerly owned by CCTA and then OGC, the BMP functions moved to the Cabinet Office in June 2010. The BMP portfolio includes guidance on IT service management and project, program, risk, portfolio, and value management. There is also a management maturity model as well as related glossaries of terms.</p>
best practice	<p>Proven activities or processes that have been successfully used by multiple organizations. ITIL® is an example of best practice.</p>
budget	<p>A list of all the money an organization or business unit plans to receive and plans to pay out over a specified period of time.</p>
	<p>See also budgeting.</p>
budgeting	<p>The activity of predicting and controlling the spending of money. Budgeting consists of a periodic negotiation cycle to set future budgets (usually annual) and the day-to-day monitoring and adjusting of current budgets.</p>
build	<p>(ITIL® Service Transition) The activity of assembling a number of configuration items to create part of an IT service. The term is also used to refer to a release that is authorized for distribution—for example, server build or laptop build.</p>
	<p>See also configuration baseline.</p>
business case	<p>(ITIL® Service Strategy) Justification for a significant item of expenditure. The business case includes information about costs, benefits, options, issues, risks, and possible problems.</p>
business continuity plan (BCP)	<p>(ITIL® Service Design) A plan defining the steps required to restore business processes following a disruption. The plan also identifies the triggers for invocation, people to be involved, communications, etc. IT service continuity plans form a significant part of business continuity plans.</p>
business impact analysis (BIA)	<p>(ITIL® Service Strategy) Business impact analysis is the activity in business continuity management that identifies vital business functions and their dependencies. These dependencies may include suppliers, people, other business processes, IT services etc. Business impact analysis defines the recovery requirements for IT services. These requirements include recovery time objectives, recovery point objectives, and minimum service level targets for each IT service.</p>

Term	Definition
business relationship management	(ITIL® Service Strategy) The process responsible for maintaining a positive relationship with customers. Business relationship management identifies customer needs and ensures that the service provider is able to meet these needs with an appropriate catalog of services. This process has strong links with service level management.
capability	(ITIL® Service Strategy) The ability of an organization, person, process, application, IT service, or other configuration item to carry out an activity. Capabilities are intangible assets of an organization.
	See also resource.
capacity	(ITIL® Service Design) The maximum throughput that a configuration item or IT service can deliver. For some types of CIs, capacity may be the size or volume—for example, a disk drive.
capacity management information system (CMIS)	(ITIL® Service Design) A set of tools, data, and information that is used to support capacity management.
capacity planning	(ITIL® Service Design) The activity within capacity management responsible for creating a capacity plan.
change	(ITIL® Service Transition) The addition, modification, or removal of anything that could have an effect on IT services. The scope should include changes to all architectures, processes, tools, metrics, and documentation, as well as changes to IT services and other configuration items.
change advisory board (CAB)	(ITIL® Service Transition) A group of people that support the assessment, prioritization, authorization, and scheduling of changes. A change advisory board is usually made up of representatives from all areas within the IT service provider, the business, and third parties, such as suppliers.
change model	(ITIL® Service Transition) A repeatable way of dealing with a particular category of change. A change model defines specific agreed steps that will be followed for a change of this category. Change models may be very complex with many steps that require authorization (e.g., major software release) or may be very simple with no requirement for authorization (e.g., password reset).
	See also change advisory board; standard change.

Term	Definition
change proposal	(ITIL® Service Strategy) (ITIL® Service Transition) A document that includes a high level description of a potential service introduction or significant change, along with a corresponding business case and an expected implementation schedule. Change proposals are normally created by the service portfolio management process and are passed to change management for authorization. Change management will review the potential impact on other services, on shared resources, and on the overall change schedule. Once the change proposal has been authorized, service portfolio management will charter the service.
change record	(ITIL® Service Transition) A record containing the details of a change. Each change record documents the lifecycle of a single change. A change record is created for every request for change that is received, even those that are subsequently rejected. Change records should reference the configuration items that are affected by the change. Change records may be stored in the configuration management system or elsewhere in the service knowledge management system.
change request	See request for change.
change schedule	(ITIL® Service Transition) A document that lists all authorized changes and their planned implementation dates, as well as the estimated dates of longer-term changes. A change schedule is sometimes called a forward schedule of change, even though it also contains information about changes that have already been implemented.
change window	(ITIL® Service Transition) A regular, agreed time when changes or releases may be implemented with minimal impact on services. Change windows are usually documented in service level agreements.
charging	(ITIL® Service Strategy) Requiring payment for IT services. Charging for IT services is optional and many organizations choose to treat their IT service provider as a cost centre.
CI type	(ITIL® Service Transition) A category that is used to classify configuration items. The CI type identifies the required attributes and relationships for a configuration record. Common CI types include hardware, document, user, etc.
classification	The act of assigning a category to something. Classification is used to ensure consistent management and reporting. Configuration items, incidents, problems, changes, etc. are usually classified.
component	A general term that is used to mean one part of something more complex. For example, a computer system may be a component of an IT service; an application may be a component of a release unit. Components that need to be managed should be configuration items.

Term	Definition
confidentiality	(ITIL® Service Design) A security principle that requires that data should only be accessed by authorized people.
configuration	(ITIL® Service Transition) A generic term used to describe a group of configuration items that work together to deliver an IT service or a recognizable part of an IT service. Configuration is also used to describe the parameter settings for one or more configuration items.
configuration baseline	(ITIL® Service Transition) The baseline of a configuration that has been formally agreed and is managed through the change management process. A configuration baseline is used as a basis for future builds, releases, and changes.
configuration item (CI)	(ITIL® Service Transition) Any component or other service asset that needs to be managed in order to deliver an IT service. Information about each configuration item is recorded in a configuration record within the configuration management system and is maintained throughout its lifecycle by service asset and configuration management. Configuration items are under the control of change management. They typically include IT services, hardware, software, buildings, people, and formal documentation, such as process documentation and service level agreements.
configuration management database (CMDB)	(ITIL® Service Transition) A database used to store configuration records throughout their lifecycle. The configuration management system maintains one or more configuration management databases, and each database stores attributes of configuration items and relationships with other configuration items.
configuration management system (CMS)	(ITIL® Service Transition) A set of tools, data, and information that is used to support service asset and configuration management. The CMS is part of an overall service knowledge management system and includes tools for collecting, storing, managing, updating, analyzing, and presenting data about all configuration items and their relationships. The CMS may also include information about incidents, problems, known errors, changes, and releases. The CMS is maintained by service asset and configuration management and is used by all IT service management processes.
See also configuration management database.	(ITIL® Service Transition) A record containing the details of a configuration item. Each configuration record documents the lifecycle of a single configuration item. Configuration records are stored in a configuration management database and maintained as part of a configuration management system.

Term	Definition
countermeasure	Can be used to refer to any type of control. The term is most often used when referring to measures that increase resilience, fault tolerance, or reliability of an IT service.
critical success factor (CSF)	Something that must happen if an IT service, process, plan, project, or other activity is to succeed. Key performance indicators are used to measure the achievement of each critical success factor. For example, a critical success factor of ‘protect IT services when making changes’ could be measured by key performance indicators such as ‘percentage reduction of unsuccessful changes’, ‘percentage reduction in changes causing incidents’, etc.
CSI register	(ITIL® Continual Service Improvement) A database or structured document used to record and manage improvement opportunities throughout their lifecycle.
customer asset	Any resource or capability of a customer. See also asset.
customer portfolio	(ITIL® Service Strategy) A database or structured document used to record all customers of the IT service provider. The customer portfolio is the business relationship manager’s view of the customers who receive services from the IT service provider. See also service catalog; service portfolio.
Data-to-Information-to-Knowledge-to-Wisdom (DIKW)	(ITIL® Service Transition) A way of understanding the relationships between data, information, knowledge, and wisdom. DIKW shows how each of these builds on the others.
definitive media library (DML)	(ITIL® Service Transition) One or more locations in which the definitive and authorized versions of all software configuration items are securely stored. The definitive media library may also contain associated configuration items, such as licenses and documentation. It is a single logical storage area, even if there are multiple locations. The definitive media library is controlled by service asset and configuration management and is recorded in the configuration management system.
Deming Cycle	See Plan-Do-Check-Act.
deployment	(ITIL® Service Transition) The activity responsible for movement of new or changed hardware, software, documentation, process, etc. to the live environment. Deployment is part of the release and deployment management process.

Term	Definition
design coordination	(ITIL® Service Design) The process responsible for coordinating all service design activities, processes, and resources. Design coordination ensures the consistent and effective design of new or changed IT services, service management information systems, architectures, technology, processes, information, and metrics.
document	Information in readable form. A document may be paper or electronic—for example, a policy statement, service level agreement, incident record, or diagram of a computer room layout.
	See also record.
downtime	(ITIL® Service Design) (ITIL® Service Operation) The time when an IT service or other configuration item is not available during its agreed service time. The availability of an IT service is often calculated from agreed service time and downtime.
emergency change	(ITIL® Service Transition) A change that must be introduced as soon as possible—for example, to resolve a major incident or implement a security patch. The change management process will normally have a specific procedure for handling emergency changes.
	See also emergency change advisory board.
emergency change advisory board (ECAB)	(ITIL® Service Transition) A subgroup of the change advisory board that makes decisions about emergency changes. Membership may be decided at the time a meeting is called and depends on the nature of the emergency change.
escalation	(ITIL® Service Operation) An activity that obtains additional resources when these are needed to meet service level targets or customer expectations. Escalation may be needed within any IT service management process but is most commonly associated with incident management, problem management, and the management of customer complaints. There are two types of escalation: functional escalation and hierachic escalation.
event	(ITIL® Service Operation) A change of state that has significance for the management of an IT service or other configuration item. The term is also used to mean an alert or notification created by any IT service, configuration item, or monitoring tool. Events typically require IT operations personnel to take actions and often lead to incidents being logged.
external customer	A customer who works for a different business from the IT service provider.
	See also external service provider; internal customer.

Term	Definition
external service provider	(ITIL® Service Strategy) An IT service provider that is part of a different organization from its customer. An IT service provider may have both internal and external customers.
	See also Type III service provider.
facilities management	(ITIL® Service Operation) The function responsible for managing the physical environment where the IT infrastructure is located. Facilities management includes all aspects of managing the physical environment—for example, power and cooling, building access management, and environmental monitoring.
failure	(ITIL® Service Operation) Loss of ability to operate to specification or to deliver the required output. The term may be used when referring to IT services, processes, activities, configuration items, etc. A failure often causes an incident.
fast recovery	(ITIL® Service Design) A recovery option that is also known as hot standby. Fast recovery normally uses a dedicated fixed facility with computer systems and software configured ready to run the IT services. Fast recovery typically takes up to 24 hours but may be quicker if there is no need to restore data from backups.
fit for purpose	(ITIL® Service Strategy) The ability to meet an agreed level of utility. Fit for purpose is also used informally to describe a process, configuration item, IT service, etc. that is capable of meeting its objectives or service levels. Being fit for purpose requires suitable design, implementation, control, and maintenance.
fit for use	(ITIL® Service Strategy) The ability to meet an agreed level of warranty. Being fit for use requires suitable design, implementation, control, and maintenance.
follow the sun	(ITIL® Service Operation) A methodology for using service desks and support groups around the world to provide seamless 24/7 service. Calls, incidents, problems, and service requests are passed between groups in different time zones.
function	A team or group of people and the tools or other resources they use to carry out one or more processes or activities—for example, the service desk. The term also has two other meanings: An intended purpose of a configuration item, person, team, process, or IT service. For example, one function of an email service may be to store and forward outgoing mails, while the function of a business process may be to dispatch goods to customers. To perform the intended purpose correctly, as in 'The computer is functioning.'

Term	Definition
functional escalation	(ITIL® Service Operation) Transferring an incident, problem, or change to a technical team with a higher level of expertise to assist in an escalation.
governance	Ensures that policies and strategy are actually implemented and that required processes are correctly followed. Governance includes defining roles and responsibilities, measuring and reporting, and taking actions to resolve any issues identified.
gradual recovery	(ITIL® Service Design) A recovery option that is also known as cold standby. Gradual recovery typically uses a portable or fixed facility that has environmental support and network cabling but no computer systems. The hardware and software are installed as part of the IT service continuity plan. Gradual recovery typically takes more than three days and may take significantly longer.
hierarchic escalation	(ITIL® Service Operation) Informing or involving more senior levels of management to assist in an escalation.
hot standby	See fast recovery; immediate recovery.
immediate recovery	(ITIL® Service Design) A recovery option that is also known as hot standby. Provision is made to recover the IT service with no significant loss of service to the customer. Immediate recovery typically uses mirroring, load balancing, and split-site technologies.
impact	(ITIL® Service Operation) (ITIL® Service Transition) A measure of the effect of an incident, problem, or change on business processes. Impact is often based on how service levels will be affected. Impact and urgency are used to assign priority.
incident	(ITIL® Service Operation) An unplanned interruption to an IT service or reduction in the quality of an IT service. Failure of a configuration item that has not yet affected service is also an incident—for example, failure of one disk from a mirror set.
incident record	(ITIL® Service Operation) A record containing the details of an incident. Each incident record documents the lifecycle of a single incident.
information security management (ISM)	(ITIL® Service Design) The process responsible for ensuring that the confidentiality, integrity, and availability of an organization's assets, information, data, and IT services match the agreed needs of the business. Information security management supports business security, has a wider scope than that of the IT service provider, and includes handling of paper, building access, phone calls, etc. for the entire organization.
information security policy	See also security management information system. (ITIL® Service Design) The policy that governs the organization's approach to information security management.

Term	Definition
information technology (IT)	The use of technology for the storage, communication, or processing of information. The technology typically includes computers, telecommunications, applications, and other software. The information may include business data, voice, images, video, etc. Information technology is often used to support business processes through IT services.
intermediate recovery	(ITIL® Service Design) A recovery option that is also known as warm standby. Intermediate recovery usually uses a shared portable or fixed facility that has computer systems and network components. The hardware and software will need to be configured and data will need to be restored as part of the IT service continuity plan. Typical recovery times for intermediate recovery are one to three days.
internal customer	A customer who works for the same business as the IT service provider.
	See also external customer; internal service provider.
internal service provider	(ITIL® Service Strategy) An IT service provider that is part of the same organization as its customer. An IT service provider may have both internal and external customers.
	See also Type I service provider; Type II service provider.
internet service provider (ISP)	An external service provider that provides access to the internet. Most ISPs also provide other IT services, such as web hosting.
ISO 9000	A generic term that refers to a number of international standards and guidelines for quality management systems.
	See www.iso.org for more information.
ISO 9001	An international standard for quality management systems.
	See also ISO 9000.
ISO/IEC 20000	An international standard for IT service management.
ISO/IEC 27001	(ITIL® Continual Service Improvement) (ITIL® Service Design) An international specification for information security management. The corresponding code of practice is ISO/IEC 27002.
ISO/IEC 27002	(ITIL® Continual Service Improvement) An international code of practice for information security management. The corresponding specification is ISO/IEC 27001.
IT accounting	See accounting.

Term	Definition
IT infrastructure	All of the hardware, software, networks, facilities, etc. that are required to develop, test, deliver, monitor, control, or support applications and IT services. The term includes all of the information technology but not the associated people, processes, and documentation.
IT operations	(ITIL® Service Operation) Activities carried out by IT operations control, including console management/operations bridge, job scheduling, backup and restore, and print and output management. IT operations is also used as a synonym for service operation.
IT operations control	(ITIL® Service Operation) The function responsible for monitoring and control of the IT services and IT infrastructure.
	See also operations bridge.
IT service	A service provided by an IT service provider. An IT service is made up of a combination of information technology, people, and processes. A customer-facing IT service directly supports the business processes of one or more customers, and its service level targets should be defined in a service level agreement. Other IT services, called supporting services, are not directly used by the business but are required by the service provider to deliver customer-facing services.
	See also service; service package.
IT service continuity plan	(ITIL® Service Design) A plan defining the steps required to recover one or more IT services. The plan also identifies the triggers for invocation, people to be involved, communications, etc. The IT service continuity plan should be part of a business continuity plan.
IT service management (ITSM)	The implementation and management of quality IT services that meet the needs of the business. IT service management is performed by IT service providers through an appropriate mix of people, process, and information technology.
	See also service management.
IT Service Management Forum (itSMF)	The IT Service Management Forum is an independent organization dedicated to promoting a professional approach to IT service management. The itSMF is a not-for-profit membership organization with representation in many countries around the world (itSMF chapters). The itSMF and its membership contribute to the development of ITIL® and associated IT service management standards.
	See www.itsmf.com for more information.

Term	Definition
IT service provider	(ITIL® Service Strategy) A service provider that provides IT services to internal or external customers.
ITIL®	<p>A set of best-practice publications for IT service management. Owned by the Cabinet Office (part of HM Government), ITIL® gives guidance on the provision of quality IT services and the processes, functions, and other capabilities needed to support them. The ITIL® framework is based on a service lifecycle and consists of five lifecycle stages (service strategy, service design, service transition, service operation, and continual service improvement), each of which has its own supporting publication. There is also a set of complementary ITIL® publications providing guidance specific to industry sectors, organization types, operating models, and technology architectures.</p>
	See www.itilofficialsite.com for more information.
key performance indicator (KPI)	(ITIL® Continual Service Improvement) (ITIL® Service Design) A metric that is used to help manage an IT service, process, plan, project, or other activity. Key performance indicators are used to measure the achievement of critical success factors. Many metrics may be measured, but only the most important of these are defined as key performance indicators and used to actively manage and report on the process, IT service, or activity. They should be selected to ensure that efficiency, effectiveness, and cost effectiveness are all managed.
known error	(ITIL® Service Operation) A problem that has a documented root cause and a workaround. Known errors are created and managed throughout their lifecycle by problem management. Known errors may also be identified by development or suppliers.
known error database (KEDB)	(ITIL® Service Operation) A database containing all known error records. This database is created by problem management and used by incident and problem management. The known error database may be part of the configuration management system or may be stored elsewhere in the service knowledge management system.
known error record	(ITIL® Service Operation) A record containing the details of a known error. Each known error record documents the lifecycle of a known error, including the status, root cause, and workaround. In some implementations, a known error is documented using additional fields in a problem record.

Term	Definition
lifecycle	<p>The various stages in the life of an IT service, configuration item, incident, problem, change, etc. The lifecycle defines the categories for status and the status transitions that are permitted. For example: The lifecycle of an application includes requirements, design, build, deploy, operate, optimize</p> <p>The expanded incident lifecycle includes detection, diagnosis, repair, recovery, and restoration</p> <p>The lifecycle of a server may include ordered, received, in test, live, disposed etc.</p>
maintainability	<p>(ITIL® Service Design) A measure of how quickly and effectively an IT service or other configuration item can be restored to normal working after a failure. Maintainability is often measured and reported as MTRS.</p> <p>Maintainability is also used in the context of software or IT service development to mean ability to be changed or repaired easily.</p>
major incident	<p>(ITIL® Service Operation) The highest category of impact for an incident. A major incident results in significant disruption to the business.</p>
manual workaround	<p>(ITIL® Continual Service Improvement) A workaround that requires manual intervention. Manual workaround is also used as the name of a recovery option in which the business process operates without the use of IT services. This is a temporary measure and is usually combined with another recovery option.</p>
modeling	<p>A technique that is used to predict the future behavior of a system, process, IT service, configuration item, etc. Modeling is commonly used in financial management, capacity management, and availability management.</p>
normal change	<p>(ITIL® Service Transition) A change that is not an emergency change or a standard change. Normal changes follow the defined steps of the change management process.</p>
operational level agreement (OLA)	<p>(ITIL® Continual Service Improvement) (ITIL® Service Design) An agreement between an IT service provider and another part of the same organization. It supports the IT service provider's delivery of IT services to customers and defines the goods or services to be provided and the responsibilities of both parties. For example, there could be an operational level agreement:</p> <p>Between the IT service provider and a procurement department to obtain hardware in agreed times</p> <p>Between the service desk and a support group to provide incident resolution in agreed times.</p>
See also service level agreement.	

Term	Definition
operations bridge	(ITIL® Service Operation) A physical location where IT services and IT infrastructure are monitored and managed.
operations control	See IT operations control.
outcome	The result of carrying out an activity, following a process, or delivering an IT service, etc. The term is used to refer to intended results as well as to actual results.
pattern of business activity (PBA)	(ITIL® Service Strategy) A workload profile of one or more business activities. Patterns of business activity are used to help the IT service provider understand and plan for different levels of business activity.
Plan-Do-Check-Act (PDCA)	(ITIL® Continual Service Improvement) A four-stage cycle for process management, attributed to Edward Deming. Plan—design or revise processes that support the IT services; Do—implement the plan and manage the processes; Check—measure the processes and IT services, compare with objectives and produce reports; Act—plan and implement changes to improve the processes.
post-implementation review (PIR)	A review that takes place after a change or a project has been implemented. It determines if the change or project was successful and identifies opportunities for improvement.
PRINCE2®	See PRojects IN Controlled Environments.
proactive problem management	(ITIL® Service Operation) Part of the problem management process. The objective of proactive problem management is to identify problems that might otherwise be missed. Proactive problem management analyzes incident records and uses data collected by other IT service management processes to identify trends or significant problems.
problem	(ITIL® Service Operation) A cause of one or more incidents. The cause is not usually known at the time a problem record is created, and the problem management process is responsible for further investigation.
problem record	(ITIL® Service Operation) A record containing the details of a problem. Each problem record documents the lifecycle of a single problem.
process	A structured set of activities designed to accomplish a specific objective. A process takes one or more defined inputs and turns them into defined outputs. It may include any of the roles, responsibilities, tools, and management controls required to reliably deliver the outputs. A process may define policies, standards, guidelines, activities, and work instructions if they are needed.

Term	Definition
process control	The activity of planning and regulating a process with the objective of performing the process in an effective, efficient, and consistent manner.
process manager	A role responsible for the operational management of a process. The process manager's responsibilities include planning and coordination of all activities required to carry out, monitor, and report on the process. There may be several process managers for one process—for example, regional change managers or IT service continuity managers for each data centre. The process manager role is often assigned to the person who carries out the process owner role, but the two roles may be separate in larger organizations.
process owner	The person who is held accountable for ensuring that a process is fit for purpose. The process owner's responsibilities include sponsorship, design, change management, and continual improvement of the process and its metrics. This role can be assigned to the same person who carries out the process manager role, but the two roles may be separate in larger organizations.
project	A temporary organization, with people and other assets, that is required to achieve an objective or other outcome. Each project has a lifecycle that typically includes initiation, planning, execution, and closure. Projects are usually managed using a formal methodology, such as PRojects IN Controlled Environments (PRINCE2) or the Project Management Body of Knowledge (PMBOK).
PRojects IN Controlled Environments (PRINCE2)	The standard UK government methodology for project management. See www.princeofficialsite.com for more information. See also Project Management Body of Knowledge (PMBOK).
Project Management Body of Knowledge (PMBOK)	A project management standard maintained and published by the Project Management Institute. See www.pmi.org for more information. See also PRojects IN Controlled Environments (PRINCE2).

Term	Definition
Project Management Institute (PMI)	<p>A membership association that advances the project management profession through globally recognized standards and certifications, collaborative communities, an extensive research program, and professional development opportunities. PMI is a not-for-profit membership organization with representation in many countries around the world. PMI maintains and publishes the Project Management Body of Knowledge (PMBOK).</p>
	<p>See www.pmi.org for more information.</p>
	<p>See also PRojects IN Controlled Environments (PRINCE2).</p>
quality	<p>The ability of a product, service, or process to provide the intended value. For example, a hardware component can be considered to be of high quality if it performs as expected and delivers the required reliability. Process quality also requires an ability to monitor effectiveness and efficiency and to improve them if necessary.</p>
	<p>See also quality management system.</p>
quality assurance (QA)	<p>(ITIL® Service Transition) The process responsible for ensuring that the quality of a service, process, or other service asset will provide its intended value. Quality assurance is also used to refer to a function or team that performs quality assurance. This process is not described in detail within the core ITIL® publications.</p>
quality management system (QMS)	<p>(ITIL® Continual Service Improvement) The framework of policy, processes, functions, standards, guidelines, and tools that ensures an organization is of a suitable quality to reliably meet business objectives or service levels.</p>
	<p>See also ISO 9000.</p>
RACI	<p>(ITIL® Service Design) A model used to help define roles and responsibilities. RACI stands for responsible, accountable, consulted and informed.</p>
reciprocal arrangement	<p>(ITIL® Service Design) A recovery option. An agreement between two organizations to share resources in an emergency—for example, high-speed printing facilities or computer room space.</p>
record	<p>A document containing the results or other output from a process or activity. Records are evidence of the fact that an activity took place and may be paper or electronic—for example, an audit report, an incident record, or the minutes of a meeting.</p>

Term	Definition
recovery	(ITIL® Service Design) (ITIL® Service Operation) Returning a configuration item or an IT service to a working state. Recovery of an IT service often includes recovering data to a known consistent state. After recovery, further steps may be needed before the IT service can be made available to the users (restoration).
recovery option	(ITIL® Service Design) A strategy for responding to an interruption to service. Commonly used strategies are manual workaround, reciprocal arrangement, gradual recovery, intermediate recovery, fast recovery, and immediate recovery. Recovery options may make use of dedicated facilities or third-party facilities shared by multiple businesses.
relationship	A connection or interaction between two people or things. In business relationship management, it is the interaction between the IT service provider and the business. In service asset and configuration management, it is a link between two configuration items that identifies a dependency or connection between them. For example, applications may be linked to the servers they run on, and IT services have many links to all the configuration items that contribute to that IT service.
release	(ITIL® Service Transition) One or more changes to an IT service that are built, tested, and deployed together. A single release may include changes to hardware, software, documentation, processes, and other components.
release package	(ITIL® Service Transition) A set of configuration items that will be built, tested, and deployed together as a single release. Each release package will usually include one or more release units.
release record	(ITIL® Service Transition) A record that defines the content of a release. A release record has relationships with all configuration items that are affected by the release. Release records may be in the configuration management system or elsewhere in the service knowledge management system.
release unit	(ITIL® Service Transition) Components of an IT service that are normally released together. A release unit typically includes sufficient components to perform a useful function. For example, one release unit could be a desktop PC, including hardware, software, licenses, documentation, etc. A different release unit may be the complete payroll application, including IT operations procedures and user training.
release window	See change window.

Term	Definition
reliability	<p>(ITIL® Continual Service Improvement) (ITIL® Service Design) A measure of how long an IT service or other configuration item can perform its agreed function without interruption. Usually measured as MTBF or MTBSI. The term can also be used to state how likely it is that a process, function, etc. will deliver its required outputs.</p> <p>See also availability.</p>
remediation	<p>(ITIL® Service Transition) Actions taken to recover after a failed change or release. Remediation may include back-out, invocation of service continuity plans, or other actions designed to enable the business process to continue.</p>
request for change (RFC)	<p>(ITIL® Service Transition) A formal proposal for a change to be made. It includes details of the proposed change and may be recorded on paper or electronically. The term is often misused to mean a change record or the change itself.</p>
request fulfillment	<p>(ITIL® Service Operation) The process responsible for managing the lifecycle of all service requests.</p>
request model	<p>(ITIL® Service Operation) A repeatable way of dealing with a particular category of service request. A request model defines specific agreed steps that will be followed for a service request of this category. Request models may be very simple with no requirement for authorization (e.g., password reset) or may be more complex with many steps that require authorization (e.g., provision of an existing IT service).</p> <p>See also request fulfillment.</p>
resilience	<p>(ITIL® Service Design) The ability of an IT service or other configuration item to resist failure or to recover in a timely manner following a failure. For example, an armored cable will resist failure when put under stress.</p>
resolution	<p>(ITIL® Service Operation) Action taken to repair the root cause of an incident or problem or to implement a workaround. In ISO/IEC 20000, resolution processes is the process group that includes incident and problem management.</p>
resource	<p>(ITIL® Service Strategy) A generic term that includes IT infrastructure, people, money, or anything else that might help to deliver an IT service. Resources are considered to be assets of an organization.</p> <p>See also capability; service asset.</p>

Term	Definition
response time	A measure of the time taken to complete an operation or transaction. Used in capacity management as a measure of IT infrastructure performance and in incident management as a measure of the time taken to answer the phone or to start diagnosis.
restoration of service	See restore.
restore	(ITIL® Service Operation) Taking action to return an IT service to the users after repair and recovery from an incident. This is the primary objective of incident management.
retire	(ITIL® Service Transition) Permanent removal of an IT service or other configuration item from the live environment. Being retired is a stage in the lifecycle of many configuration items.
return on investment (ROI)	(ITIL® Continual Service Improvement) (ITIL® Service Strategy) A measurement of the expected benefit of an investment. In the simplest sense, it is the net profit of an investment divided by the net worth of the assets invested.
rights	(ITIL® Service Operation) Entitlements or permissions granted to a user or role—for example, the right to modify particular data or to authorize a change.
risk	A possible event that could cause harm or loss or affect the ability to achieve objectives. A risk is measured by the probability of a threat, the vulnerability of the asset to that threat, and the impact it would have if it occurred. Risk can also be defined as uncertainty of outcome and can be used in the context of measuring the probability of positive outcomes as well as negative outcomes.
risk assessment	The initial steps of risk management: analyzing the value of assets to the business, identifying threats to those assets, and evaluating how vulnerable each asset is to those threats. Risk assessment can be quantitative (based on numerical data) or qualitative.
risk management	The process responsible for identifying, assessing, and controlling risks. Risk management is also sometimes used to refer to the second part of the overall process after risks have been identified and assessed, as in ‘risk assessment and management’. This process is not described in detail within the core ITIL® publications.

See also risk assessment.

Term	Definition
role	A set of responsibilities, activities, and authorities assigned to a person or team. A role is defined in a process or function. One person or team may have multiple roles—for example, the roles of configuration manager and change manager may be carried out by a single person. Role is also used to describe the purpose of something or what it is used for.
root cause	(ITIL® Service Operation) The underlying or original cause of an incident or problem.
scope	The boundary or extent to which a process, procedure, certification, contract, etc. applies. For example, the scope of change management may include all live IT services and related configuration items; the scope of an ISO/IEC 20000 certificate may include all IT services delivered out of a named data centre.
security	See information security management.
security management information system (SMIS)	(ITIL® Service Design) A set of tools, data, and information that is used to support information security management. The security management information system is part of the information security management system.
	See also service knowledge management system.
security policy	See information security policy.
service	A means of delivering value to customers by facilitating outcomes customers want to achieve without the ownership of specific costs and risks. The term 'service' is sometimes used as a synonym for core service, IT service, or service package.
	See also utility; warranty.
service asset	Any resource or capability of a service provider.
	See also asset.
service capacity management (SCM)	(ITIL® Continual Service Improvement) (ITIL® Service Design) The sub-process of capacity management responsible for understanding the performance and capacity of IT services. Information on the resources used by each IT service and the pattern of usage over time are collected, recorded, and analyzed for use in the capacity plan.
service catalog	(ITIL® Service Design) (ITIL® Service Strategy) A database or structured document with information about all live IT services, including those available for deployment. The service catalog 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.

Term	Definition
service contract	(ITIL® Service Strategy) A contract to deliver one or more IT services. The term is also used to mean any agreement to deliver IT services, whether this is a legal contract or a service level agreement.
service design package (SDP)	(ITIL® Service Design) Document(s) defining all aspects of an IT service and its requirements through each stage of its lifecycle. A service design package is produced for each new IT service, major change, or IT service retirement.
service desk	(ITIL® Service Operation) The single point of contact between the service provider and the users. A typical service desk manages incidents and service requests and also handles communication with the users.
service improvement plan (SIP)	(ITIL® Continual Service Improvement) A formal plan to implement improvements to a process or IT service.
service knowledge management system (SKMS)	(ITIL® Service Transition) A set of tools and databases that is used to manage knowledge, information, and data. The service knowledge management system includes the configuration management system, as well as other databases and information systems. The service knowledge management system includes tools for collecting, storing, managing, updating, analyzing, and presenting all the knowledge, information, and data that an IT service provider will need to manage the full lifecycle of IT services.
service level	Measured and reported achievement against one or more service level targets. The term is sometimes used informally to mean service level target.
service level agreement (SLA)	(ITIL® Continual Service Improvement) (ITIL® Service Design) An agreement between an IT service provider and a customer. A service level agreement describes the IT service, documents service level targets, and specifies the responsibilities of the IT service provider and the customer. A single agreement may cover multiple IT services or multiple customers.
service level package (SLP)	See also operational level agreement.
service level requirement (SLR)	(ITIL® Continual Service Improvement) (ITIL® Service Design) A customer requirement for an aspect of an IT service. Service level requirements are based on business objectives and used to negotiate agreed service level targets.
service management	(ITIL® Service Operation) The expected time that a configuration item will be unavailable due to planned maintenance activity.

Term	Definition
service manager	A generic term for any manager within the service provider. Most commonly used to refer to a business relationship manager, a process manager, or a senior manager with responsibility for IT services overall.
service model	(ITIL® Service Strategy) A model that shows how service assets interact with customer assets to create value. Service models describe the structure of a service (how the configuration items fit together) and the dynamics of the service (activities, flow of resources, and interactions). A service model can be used as a template or blueprint for multiple services.
service option	(ITIL® Service Design) (ITIL® Service Strategy) A choice of utility and warranty offered to customers by a core service or service package. Service options are sometimes referred to as service level packages.
service owner	(ITIL® Service Strategy) A role responsible for managing one or more services throughout their entire lifecycle. Service owners are instrumental in the development of service strategy and are responsible for the content of the service portfolio.
service package	(ITIL® Service Strategy) Two or more services that have been combined to offer a solution to a specific type of customer need or to underpin specific business outcomes. A service package can consist of a combination of core services, enabling services and enhancing services. A service package provides a specific level of utility and warranty. Customers may be offered a choice of utility and warranty through one or more service options.
See also IT service.	
service pipeline	(ITIL® Service Strategy) A 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.
service portfolio	(ITIL® Service Strategy) The 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 catalog (live or available for deployment), and retired services.
service provider	(ITIL® Service Strategy) An organization supplying services to one or more internal customers or external customers. Service provider is often used as an abbreviation for IT service provider.
See also Type I service provider; Type II service provider; Type III service provider.	

Term	Definition
service reporting	(ITIL® Continual Service Improvement) Activities that produce and deliver reports of achievement and trends against service levels. The format, content, and frequency of reports should be agreed with customers.
service request	(ITIL® Service Operation) A formal request from a user for something to be provided—for example, a request for information or advice, to reset a password, or to install a workstation for a new user. Service requests are managed by the request fulfillment process, usually in conjunction with the service desk. Service requests may be linked to a request for change as part of fulfilling the request.
serviceability	(ITIL® Continual Service Improvement) (ITIL® Service Design) The ability of a third-party supplier to meet the terms of its contract. This contract will include agreed levels of reliability, maintainability, and availability for a configuration item.
seven-step improvement process	(ITIL® Continual Service Improvement) The process responsible for defining and managing the steps needed to identify, define, gather, process, analyze, present, and implement improvements. The performance of the IT service provider is continually measured by this process and improvements are made to processes, IT services, and IT infrastructure in order to increase efficiency, effectiveness, and cost effectiveness. Opportunities for improvement are recorded and managed in the CSI register.
shared service unit	See Type II service provider.
single point of contact	(ITIL® Service Operation) Providing a single consistent way to communicate with an organization or business unit. For example, a single point of contact for an IT service provider is usually called a service desk.
SLAM chart	(ITIL® Continual Service Improvement) A service level agreement monitoring chart is used to help monitor and report achievements against service level targets. A SLAM chart is typically color-coded to show whether each agreed service level target has been met, missed, or nearly missed during each of the previous 12 months.
stakeholder	A person who has an interest in an organization, project, IT service, etc. Stakeholders may be interested in the activities, targets, resources, or deliverables. Stakeholders may include customers, partners, employees, shareholders, owners, etc.
See also RACI.	

Term	Definition
standard change	(ITIL® Service Transition) A pre-authorized change that is low risk, relatively common, and follows a procedure or work instruction—for example, a password reset or provision of standard equipment to a new employee. Requests for change are not required to implement a standard change, and they are logged and tracked using a different mechanism, such as a service request.
	See also change model.
status accounting	(ITIL® Service Transition) The activity responsible for recording and reporting the lifecycle of each configuration item.
strategic asset	(ITIL® Service Strategy) Any asset that provides the basis for core competence, distinctive performance, or sustainable competitive advantage or that allows a business unit to participate in business opportunities. Part of service strategy is to identify how IT can be viewed as a strategic asset rather than an internal administrative function.
super user	(ITIL® Service Operation) A user who helps other users and assists in communication with the service desk or other parts of the IT service provider. Super users are often experts in the business processes supported by an IT service and will provide support for minor incidents and training.
supplier	(ITIL® Service Design) (ITIL® Service Strategy) A third party responsible for supplying goods or services that are required to deliver IT services. Examples of suppliers include commodity hardware and software vendors, network and telecom providers, and outsourcing organizations.
	See also underpinning contract.
supplier and contract management information system (SCMIS)	(ITIL® Service Design) A set of tools, data, and information that is used to support supplier management.
	See also service knowledge management system.
technical management	(ITIL® Service Operation) The function responsible for providing technical skills in support of IT services and management of the IT infrastructure. Technical management defines the roles of support groups, as well as the tools, processes, and procedures required.
test	(ITIL® Service Transition) An activity that verifies that a configuration item, IT service, process, etc. meets its specification or agreed requirements.

Term	Definition
third party	<p>A person, organization, or other entity that is not part of the service provider's own organization and is not a customer—for example, a software supplier or a hardware maintenance company. Requirements for third parties are typically specified in contracts that underpin service level agreements.</p> <p>See also underpinning contract.</p>
third-line support	<p>(ITIL® Service Operation) The third level in a hierarchy of support groups involved in the resolution of incidents and investigation of problems. Each level contains more specialist skills, or has more time or other resources.</p>
threat	<p>A threat is anything that might exploit a vulnerability. Any potential cause of an incident can be considered a threat. For example, a fire is a threat that could exploit the vulnerability of flammable floor coverings.</p> <p>This term is commonly used in information security management and IT service continuity management but also applies to other areas, such as problem and availability management.</p>
transition	<p>(ITIL® Service Transition) A change in state, corresponding to a movement of an IT service or other configuration item from one lifecycle status to the next.</p>
trend analysis	<p>(ITIL® Continual Service Improvement) Analysis of data to identify time-related patterns. Trend analysis is used in problem management to identify common failures or fragile configuration items and in capacity management as a modeling tool to predict future behavior. It is also used as a management tool for identifying deficiencies in IT service management processes.</p>
tuning	<p>The activity responsible for planning changes to make the most efficient use of resources. Tuning is most commonly used in the context of IT services and components. Tuning is part of capacity management, which also includes performance monitoring and implementation of the required changes. Tuning is also called optimization, particularly in the context of processes and other nontechnical resources.</p>
Type I service provider	<p>(ITIL® Service Strategy) An internal service provider that is embedded within a business unit. There may be several Type I service providers within an organization.</p>
Type II service provider	<p>(ITIL® Service Strategy) An internal service provider that provides shared IT services to more than one business unit. Type II service providers are also known as shared service units.</p>
Type III service provider	<p>(ITIL® Service Strategy) A service provider that provides IT services to external customers.</p>

Term	Definition
underpinning contract (UC)	(ITIL® Service Design) A contract between an IT service provider and a third party. The third party provides goods or services that support delivery of an IT service to a customer. The underpinning contract defines targets and responsibilities that are required to meet agreed service level targets in one or more service level agreements.
urgency	(ITIL® Service Design) (ITIL® Service Transition) A measure of how long it will be until an incident, problem, or change has a significant impact on the business. For example, a high-impact incident may have low urgency if the impact will not affect the business until the end of the financial year. Impact and urgency are used to assign priority.
user	A person who uses the IT service on a day-to-day basis. Users are distinct from customers, as some customers do not use the IT service directly.
utility	(ITIL® Service Strategy) The functionality offered by a product or service to meet a particular need. Utility can be summarized as ‘what the service does’ and can be used to determine whether a service is able to meet its required outcomes or is fit for purpose. The business value of an IT service is created by the combination of utility and warranty.
validation	(ITIL® Service Transition) An activity that ensures a new or changed IT service, process, plan, or other deliverable meets the needs of the business. Validation ensures that business requirements are met even though these may have changed since the original design.
verification and audit	(ITIL® Service Transition) The activities responsible for ensuring that information in the configuration management system is accurate and that all configuration items have been identified and recorded. Verification includes routine checks that are part of other processes—for example, verifying the serial number of a desktop PC when a user logs an incident. Audit is a periodic, formal check.
vision	A description of what the organization intends to become in the future. A vision is created by senior management and is used to help influence culture and strategic planning.
vital business function (VBF)	(ITIL® Service Design) Part of a business process that is critical to the success of the business. Vital business functions are an important consideration of business continuity management, IT service continuity management, and availability management.

Term	Definition
vulnerability	A weakness that could be exploited by a threat—for example, an open firewall port, a password that is never changed, or a flammable carpet. A missing control is also considered to be a vulnerability.
warm standby	See intermediate recovery.
warranty	(ITIL® Service Strategy) Assurance that a product or service will meet agreed requirements. This may be a formal agreement, such as a service level agreement or contract, or it may be a marketing message or brand image. Warranty refers to the ability of a service to be available when needed, to provide the required capacity, and to provide the required reliability in terms of continuity and security. Warranty can be summarized as ‘how the service is delivered’ and can be used to determine whether a service is fit for use. The business value of an IT service is created by the combination of utility and warranty.
work instruction	A document containing detailed instructions that specify exactly what steps to follow to carry out an activity. A work instruction contains much more detail than a procedure and is only created if very detailed instructions are needed.
work order	A formal request to carry out a defined activity. Work orders are often used by change management and by release and deployment management to pass requests to technical management and application management functions.
workaround	(ITIL® Service Operation) Reducing or eliminating the impact of an incident or problem for which a full resolution is not yet available—for example, by restarting a failed configuration item. Workarounds for problems are documented in known error records. Workarounds for incidents that do not have associated problem records are documented in the incident record.

ABBREVIATIONS

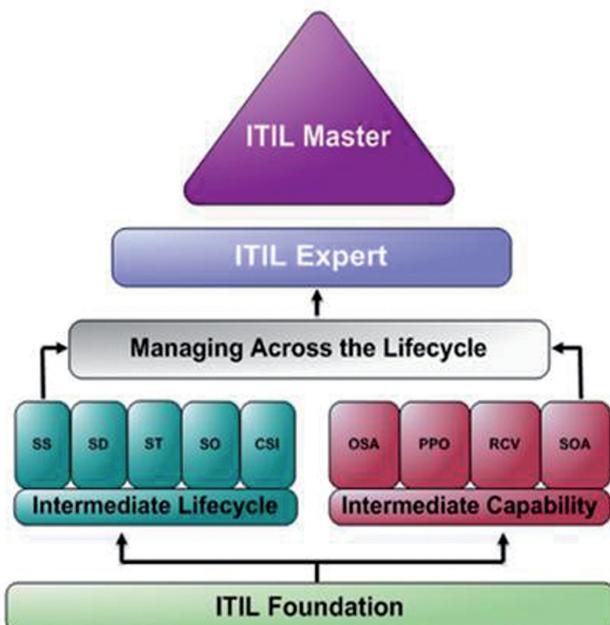
Abbreviation	Term
AMIS	Availability management information system
BCM	Business continuity management
BCP	Business continuity plan
BIA	Business impact analysis
BRM	Business relationship manager
CAB	Change advisory board
CI	Configuration item
CMDB	Configuration management database
CMIS	Capacity management information system
CMS	Configuration management system
CSF	Critical success factor
CSI	Continual service improvement
DIKW	Data-to-Information-Knowledge-to-Wisdom
DML	Definitive media library
ECAB	Emergency change advisory board
ISM	Information security management
ISMS	Information security management system
ISP	Internet service provider
IT	Information technology
ITSCM	IT service continuity management
ITSM	IT service management
ITSMF	IT service management forum
KEDB	Known error database
KPI	Key performance indicator
OLA	Operational level agreement
PBA	Pattern of business activity
PDCA	Plan-do-check-act
PIR	Post-implementation review
PMBOK	Project management body of knowledge
PMI	Project management institute

Abbreviation	Term
PRINCE2	Projects in controlled environments
PSO	Projected service outage
QMS	Quality management system
RACI	Responsible, accountable, consulted, and informed
RFC	Request for change
ROI	Return on investment
SACM	Service asset and configuration management
SCMIS	Supplier and contract management information system
SDP	Service design package
SIP	Service improvement plan
SKMS	Service knowledge management system
SLA	Service level agreement
SLM	Service level management
SLP	Service level package
SLR	Service level requirement
SMART	Specific, measurable, achievable, relevant, and time-bound
SMIS	Security management information system
UC	Underpinning contract
VBF	Vital business function
VOI	Value on investment

CERTIFICATION

ITIL® Certification Pathways

There are many pathway options that are available once you have acquired your ITIL® Foundation Certification. Below illustrates the possible pathways that are available to you. Currently it is intended that the highest certification is the ITIL® V3 Expert, considered to be equal to that of Diploma Status.



© APM Group-The Accreditor Limited 2011

Figure 12.A—ITIL® Certification Pathway

For more information on certification and available programs, please visit our website: <http://theartofservice.com>

ISO/IEC 20000 Pathways

ISO/IEC 20000 STANDARD IS BECOMING a basic requirement for IT service providers and is fast becoming the most recognized symbol of quality regarding IT Service Management processes. Once you have acquired your ITIL® Foundation Certification, you are eligible to pursue the ISO/IEC 20000 certification pathways. ISO/IEC 20000 programs aim to assist IT professionals master and understand the standard and issues relating to earning standards compliance.

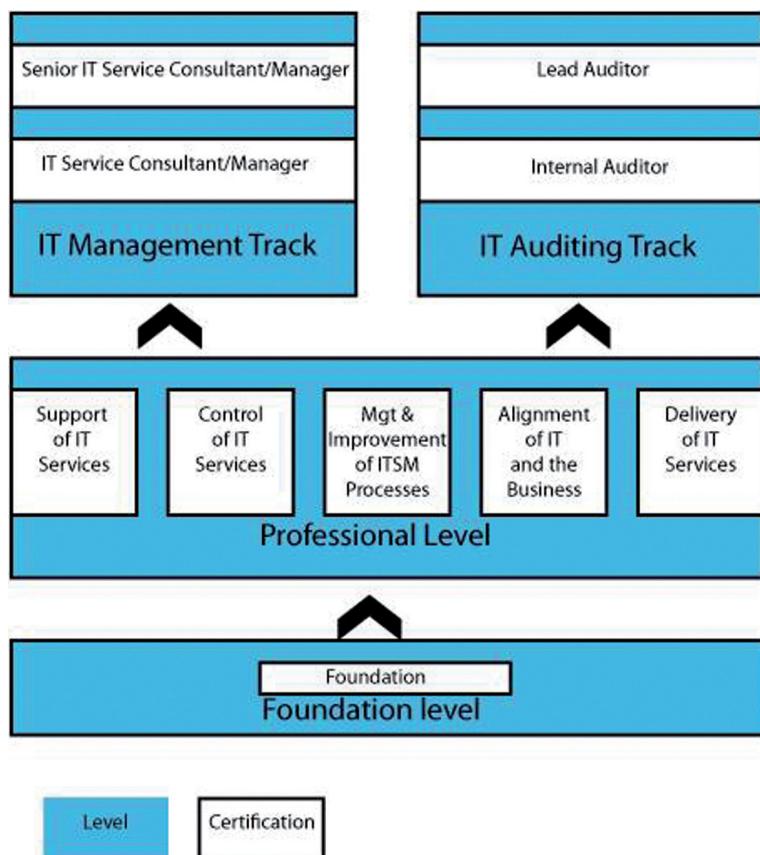


Figure 12.B—ISO/IEC 20000 Certification Pathway

For more information on certification and available programs, please visit our website: <http://theartofservice.com>

Chapter 12

INDEX

A

Access Management 250-2, 260

AMIS (availability management information system) 115, 125-6, 301, 328

Availability Management 117-20

availability management information system see AMIS

B

BCM (Business Continuity Management) 120, 126

BIA (Business impact analysis) 49, 87, 105, 128, 132, 302

BRMs (business relationship manager) 56-7

business impact analysis 49, 132

Business impact analysis see BIA

Business Relationship Management 43, 56-60

business relationship manager (BRMs) 56-7

Business Continuity Management (BCM) 120, 126

C

- CAB (Change Advisory Board) 172, 181-2, 303
- Capability Maturity Model Integrated (CMMI) 16
- Change Advisory Board (CAB) 172, 181-2, 303
- Change Management 150, 195, 293
- ClIs 102, 164-6, 219
- CMDB 162-3, 166, 300, 305
- CMMI (Capability Maturity Model Integrated) 16
- CMS (configuration management system) 77, 87, 99, 113, 134, 143, 162-4, 186, 219, 300, 305
- configuration item 106, 307-8, 313
- configuration management system see CMS
- Continual Service Improvement 8-9, 16, 50, 79, 106, 115-16
- Continuous Service Improvement see CSI
- CSI (Continuous Service Improvement) 32, 62, 264, 276, 282-3, 298-9

D

Data-to-Information-to-Knowledge-to-Wisdom see DIKW

DIKW (Data-to-Information-to-Knowledge-to-Wisdom) 156, 158, 292, 306

F

Financial Management 14, 43-7, 285

I

IT service continuity management 116, 129, 326

Incident Management 14, 28, 222, 224-5, 240

incidents 28, 30, 33, 163, 223, 226-7, 229, 236, 240, 242, 294, 305, 309, 313

Information Security Management System (ISMS) 17, 139

Internet Service Provider see ISP

Internet Service Providers 37, 39

ISMS (Information Security Management System) 17, 139

ISO/IEC 9, 17, 331

ISP (Internet Service Provider) 37-41, 310

IT Service Management see ITSM

ITSCM (IT Service Continuity Management) 120, 126, 133, 135

ITSM (IT Service Management) 1, 6-7, 11-15, 17, 19-20, 29, 36, 69, 287, 311

ITSM processes 13, 15, 43

K

KPIs (key performance indicator) 272, 275, 312

M

Mean Time Between Failures (MTBF) 123, 149, 290

Mean Time to Restore Service see MTRS

MeanTimetoRestoreService 149, 290

MTBF (Mean Time Between Failures) 123, 149, 290

MTRS (Mean Time to Restore Service) 123, 149, 290

P

PMBOK 315-16

PRINCE2 314-16

Problem Management 224, 236, 238, 240

Process Owner 20

public frameworks 16

R

RACI Model 27-8

Release and Deployment Management 150, 178, 195, 293

Return on Investment see ROI

RFCs 87, 105, 173, 177-8, 250, 253, 261, 295, 318

ROI (Return on Investment) 50, 54, 280, 319

S

SCMIS (supplier and contract management information system) 89-90, 92-4, 99, 324, 329

SDP (Service Design Package) 72, 190, 321

service catalog 50-1, 87, 104

Service Continuity Management 126, 132, 288

Service Desk 19, 22, 28, 200, 208, 234, 293, 296

Service Improvement Plans 19, 33, 86

Service Level Management 14, 56-8, 78, 289-90, 296

Service Level Package 67, 288

Service Level Packages 39-41, 288

Service Portfolio 270

Service Lifecycle 6, 20, 29-30, 34, 36, 43, 59, 61, 270

service management 1, 11-13, 15, 17, 22, 30, 34, 46

Service Measurement 273, 298

Service Operation 7, 9, 16, 27, 115, 269

service owner 20, 22, 58, 287

Service Packages 39-41, 288

Service Portfolio Management 43, 49-51, 58-9

Service Strategy 6, 8, 16, 34-6, 42-3, 45, 50, 57, 60-1, 63, 89, 101, 287

Service Support Package 67, 288

Service Transition 7, 9, 16, 50, 254, 297

Service Utility 38

Service Warranty 38

SIP (service improvement plan) 79, 86, 88, 194, 270, 292, 321

SKMS (service knowledge management system) 155-7, 161, 272, 321

SLM (Service Level Management) 73, 78, 80, 289

Supporting Service Package 67, 288 Service asset 35, 42, 54, 125

U

UC (underpinning contract) 80, 89, 326

underpinning contract see UC

utility 40-1, 286, 326

W

warranty 2, 40-1, 80, 286, 327

