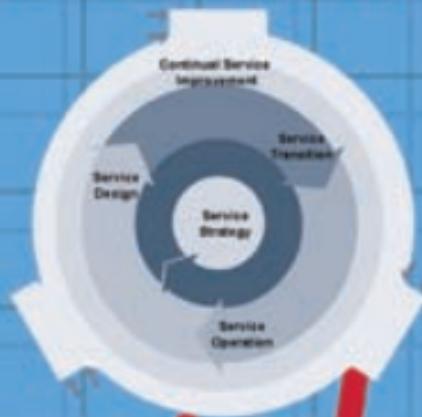




**the art of
service**

ITIL® V3 Foundation Complete Certification Kit: 2009 Edition



Study Guide Book and Online Course

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 version 3 refresh of the ITIL® framework. The evolution of the core principles and practices 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 had 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 course provided by The Art of Service. The interactive eLearn course uses a combination of narrated PowerPoint presentations with flat text supplements and multiple choice assessments. This book provides added value to the eLearn course 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 certification exam. This edition has also included appropriate alterations based on recent changes to the ITIL V3 Foundation syllabus and the associated exams.

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

The Art of Service

© The Art of Service Pty Ltd 2009

‘All of the information in this document is subject to copyright. No part of this document may in any form or by any means (whether electronic or mechanical or otherwise) be copied, reproduced, stored in a retrieval system, transmitted or provided to any other person without the prior written permission of The Art of Service Pty Ltd, who owns the copyright.’

ITIL® is a Registered Community Trade Mark of OGC (Office of Government Commerce, London, UK), and is Registered in the U.S. Patent and Trademark Office.

How to Access the eLearning Program

1. Direct your browser to: www.theartofservice.org
2. Click 'login' (found at the top right of the page)
3. Click 'Create New Account'
4. 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.
5. Once your account has been confirmed, email your User-ID for your new account to elearningbook@theartofservice.com
6. 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 login to the site, access the program titled: *ITIL V3 Foundation eLearning Program*
7. If you have any difficulties using the program or enrolling please email elearning-support@artofservice.com.au

eLearning Program: Minimum System Requirements

Processor : Pentium 4 (1 GHz) or higher

RAM : 256MB (512 MB recommended)

OS : Windows XP, Vista, MCE, Mac OSX

Browser : Macromedia Firefox 3+ (recommended), Internet Explorer 6.x or higher, Safari, Opera, Chrome, all with cookies and JavaScript enabled.

Plug-Ins : Macromedia 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 ensure that:

1. You have the latest version of Flash Player installed, by visiting <http://www.adobe.com/software/flash/about/>;
2. The security settings in your web browser don't prevent these flash modules playing; and
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

Foreword.....	1
How to Access the eLearning Program.....	2
<i>eLearning Program: Minimum System Requirements.....</i>	2
1 Introduction	7
1.1 <i>The Four Perspectives (Attributes) of ITSM</i>	8
1.2 <i>Benefits of ITSM</i>	9
1.3 <i>Business and IT Alignment.....</i>	9
1.4 <i>What is ITIL®?.....</i>	11
2 Common Terminology.....	12
2.1 <i>What are Services?.....</i>	15
2.2 <i>Processes & Functions</i>	16
2.2.1 Defining Processes	16
2.2.2 Defining Functions	18
2.2.3 Connecting Processes and Functions	19
3 The Service Lifecycle.....	20
3.1 <i>Mapping the Concepts of ITIL® to the Service Lifecycle.....</i>	22
3.2 <i>How does the Service Lifecycle work?</i>	24
4 Service Strategy.....	25
4.1 <i>Objectives</i>	25
4.2 <i>Major Concepts</i>	26
4.2.1 Creating Service Value	26
4.2.2 Service Packages and Service Level Packages.....	27
4.3 <i>Service Strategy Processes</i>	29
4.3.1 Service Portfolio Management	29
4.3.2 Financial Management	34
4.3.3 Demand Management	37
4.4 <i>Service Strategy Summary.....</i>	40
4.4.1 Interfaces with the Service Design Phase	40
4.4.2 Interfaces with the Service Transition Phase	40
4.4.3 Interfaces with the Service Operation Phase.....	41
4.4.4 Interfaces with the Continual Service Improvement Phase.....	41
4.5 <i>Service Strategy Service Scenario</i>	42
4.5.1 Overall Service Strategy	42
4.5.2 Service Portfolio Management Considerations	42
4.5.3 Financial Management Considerations	43

4.5.4	Demand Management Considerations	43
4.6	<i>Service Strategy Review Questions</i>	44
4.6.1	Question 1.....	44
4.6.2	Question 2.....	44
4.6.3	Question 3.....	44
4.6.4	Question 4.....	44
4.6.5	Question 5.....	45
4.6.6	Question 6.....	45
4.6.7	Question 7.....	45
4.6.8	Question 8.....	45
4.6.9	Question 9.....	46
4.6.10	Question 10	46
5	Service Design	47
5.1	<i>Objectives</i>	47
5.2	<i>Major Concepts</i>	48
5.2.1	Five Major Aspects of Service Design	48
5.2.2	Service Design Packages	48
5.3	<i>Service Design Processes</i>	49
5.3.1	Service Level Management	50
5.3.2	Supplier Management	55
5.3.3	Service Catalogue Management	59
5.3.4	Capacity Management	62
5.3.5	Availability Management	66
5.3.6	IT Service Continuity Management.....	71
5.3.7	Information Security Management.....	75
5.4	<i>Service Design Summary</i>	79
5.5	<i>Service Design Scenario</i>	80
5.5.1	Service Level Management Considerations	80
5.5.2	Capacity Management Considerations	80
5.5.3	Availability Management Considerations	80
5.5.4	Information Security Management Considerations.....	80
5.5.5	Service Catalogue Management Considerations	81
5.5.6	ITSCM Considerations	81
5.5.7	Supplier Management Considerations	81
5.6	<i>Service Design Review Questions</i>	82
5.6.1	Question 1.....	82
5.6.2	Question 2.....	82
5.6.3	Question 3.....	82
5.6.4	Question 4.....	82
5.6.5	Question 5.....	83
5.6.6	Question 6.....	83
5.6.7	Question 7.....	83
5.6.8	Question 8.....	83
5.6.9	Question 9.....	84
5.6.10	Question 10	84
6	Service Transition.....	85
6.1	<i>Objectives</i>	85

6.2 <i>Service Transition Processes</i>	86
6.2.1 Knowledge Management.....	86
6.2.2 Service Asset and Configuration Management.....	89
6.2.3 Change Management.....	94
6.2.4 Release and Deployment Management.....	102
6.2.5 Service Validation and Testing	107
6.3 <i>Service Transition Summary</i>	109
6.4 <i>Service Transition Scenario</i>	110
6.4.1 Knowledge Management Considerations.....	110
6.4.2 Service Asset and Configuration Management Considerations.....	110
6.4.3 Change Management Considerations.....	110
6.4.4 Release and Deployment Management Considerations.....	110
6.4.5 Service Validation and Testing Considerations.....	110
6.5 <i>Service Transition Review Questions</i>	111
6.5.1 Question 1.....	111
6.5.2 Question 2.....	111
6.5.3 Question 3.....	111
6.5.4 Question 4.....	111
6.5.5 Question 5.....	112
6.5.6 Question 6.....	112
6.5.7 Question 7.....	112
6.5.8 Question 8.....	112
6.5.9 Question 9.....	113
6.5.10 Question 10	113
7 <i>Service Operation</i>	114
7.1 <i>Objectives</i>	114
7.2 <i>Major Concepts</i>	115
7.3 <i>Service Operation Functions</i>	117
7.3.1 The Service Desk	118
7.3.2 Technical Management.....	121
7.3.3 IT Operations Management.....	123
7.3.4 Application Management	125
7.4 <i>Service Operation Processes</i>	126
7.4.1 Event Management.....	127
7.4.2 Incident Management.....	129
7.4.3 Problem Management	134
7.4.4 Request Fulfillment.....	139
7.4.5 Access Management	141
7.5 <i>Service Operation Summary</i>	142
7.6 <i>Service Operation Scenario</i>	143
7.6.1 Functions.....	143
7.6.2 Processes	143
7.7 <i>Service Operation Review Questions</i>	144
7.7.1 Question 1.....	144
7.7.2 Question 2.....	144
7.7.3 Question 3.....	144
7.7.4 Question 4.....	144

7.7.5	Question 5.....	145
7.7.6	Question 6.....	145
7.7.7	Question 7.....	145
7.7.8	Question 8.....	145
7.7.9	Question 9.....	146
7.7.10	Question 10	146
8	Continual Service Improvement.....	147
8.1	<i>Objectives</i>	147
8.2	<i>Major Concepts</i>	148
8.3	<i>Continual Service Improvement Processes</i>	149
8.3.1	Service Level Management.....	149
8.3.2	Service Measurement and Reporting	152
8.3.3	CSI (7 Step) Improvement Process.....	154
8.4	<i>Continual Service Improvement Summary</i>	156
8.5	<i>Continual Service Improvement Scenario</i>	157
8.5.1	Service Level Management.....	157
8.5.2	Service Measurement and Reporting	157
8.5.3	CSI Process	157
8.6	<i>Continual Service Improvement Review Questions</i>	158
8.6.1	Question 1.....	158
8.6.2	Question 2.....	158
8.6.3	Question 3.....	158
8.6.4	Question 4.....	158
8.6.5	Question 5.....	159
9	ITIL® Foundation Exam Tips.....	160
9.1	<i>Exam Details</i>	160
9.2	<i>Practical Suggestions</i>	160
10	Answers to Review Questions	161
10.1	<i>Service Strategy</i>	161
10.2	<i>Service Design</i>	161
10.3	<i>Service Transition</i>	161
10.4	<i>Service Operation</i>	161
10.5	<i>Continual Service Improvement</i>	161
11	Glossary	162
12	Certification	164
12.1	<i>ITIL® Certification Pathways</i>	164
12.2	<i>ISO/IEC 20000 Pathways</i>	165
13	INDEX	166

1 Introduction

The term IT Service Management (ITSM) is used in many ways by different management frameworks and organizations seeking governance and increased maturity of their IT organization. Standard elements for most definitions of ITSM include:

- Description of the **processes** required to deliver and support IT Services for customers.
- The purpose primarily being to deliver and support 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 involved.
- 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 11), describing ITSM as “**A set of specialized organizational capabilities for providing value to customers in the form of services**”. These 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.

Figure 1.A – Four Perspectives (Attributes) of ITSM

ITIL® V3 Foundation Complete Certification Kit, 2009 Edition
There are four perspectives ("4Ps") or attributes to explain the concept of ITSM.

- **Partners/Suppliers Perspective:** Takes into account the importance of Partner and External Supplier relationships and how they contribute to Service Delivery.
- **People Perspective:** Concerned with the "soft" side – IT staff, customers and other stakeholders e.g. do staff have the correct skills and knowledge to perform their roles?
- **Products/Technology Perspective:** Takes into account IT services, hardware & software budgets, tools.
- **Process Perspective:** Relates the end-to-end delivery of service based on process flows.

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 themselves, in that these four perspectives need to be considered and catered for in order to enable success in its design, transition and eventual adoption by customers.



1.2 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
- services that meet business, customer and user demands
- integrated centralized processes
- everyone knows their role and knows their responsibilities in service provision
- learning from previous experience
- demonstrable performance indicators.

It is important to consider the range of stakeholders who can benefit from improved ITSM practices. These stakeholders can come from:

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

1.3 Business and IT Alignment

A central concept to keep in mind when discussing the benefits of IT Service Management is the goal of business and IT alignment. When staff members of an IT organization have 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. A way in which to communicate how IT supports the business is using Figure 1.B, demonstrating business and IT alignment.

Figure 1.B 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:

1. **Organization:** What are the key goals for the organization?
2. **CORE Business Processes:** These business processes enable the objectives above to be met.
3. **IT Service Organization:** What IT Services are required to enable the effective and efficient execution of the business processes above?
4. **IT Service Management:** The focus here is on the ITIL® processes required for quality delivery and support of the IT Services above.
5. **IT Technical Activities:** The actual technical activities required as part of the execution of the ITIL® processes above. These are technology specific and as such not the focus of ITIL® or this document.

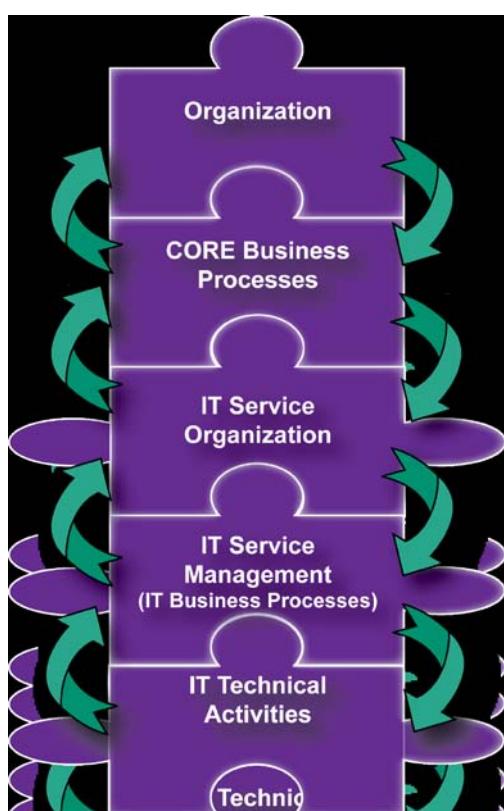


Figure 1.B – Business and IT Alignment

Example to illustrate business and IT alignment:

Our Business: A fashion store

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

- We want to make a lot of money \$\$\$!
- We want to have a good image and reputation

What Business Processes aide in achieving those objectives?
Retail, marketing, buying, procurement, HR etc.

What IT Services are these business processes dependent on?

Web site, email, automatic procurement system for buying products, Point of Sale Services

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

- What we need (Service Level 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. If this occurs we cannot adequately support our business processes effectively and efficiently. And therefore we cannot meet or support our overall organization's objectives!!!

1.4 What is ITIL®?

ITIL® stands for the Information Technology Infrastructure Library. ITIL® is the international de facto management framework describing “good 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 with the release of version 3 in 2007. 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 best practices, including those documented by:

- **Public frameworks** (ITIL®, COBIT, CMMI etc.).
- **Standards** (ISO 20000, BS 15000).
- **Proprietary knowledge of organizations and individuals.**

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

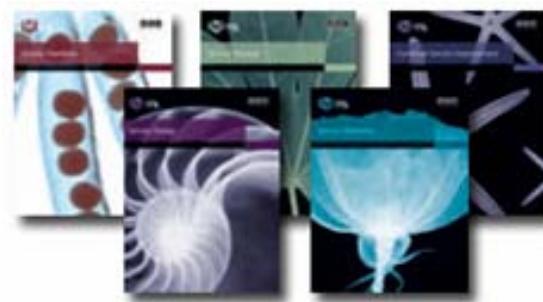


Figure 1.C – The five volumes making up the ITIL framework

Five volumes make up the IT Infrastructure Library (Version 3):

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

2 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 next section documents the important common terminology that is used throughout the ITIL® framework.

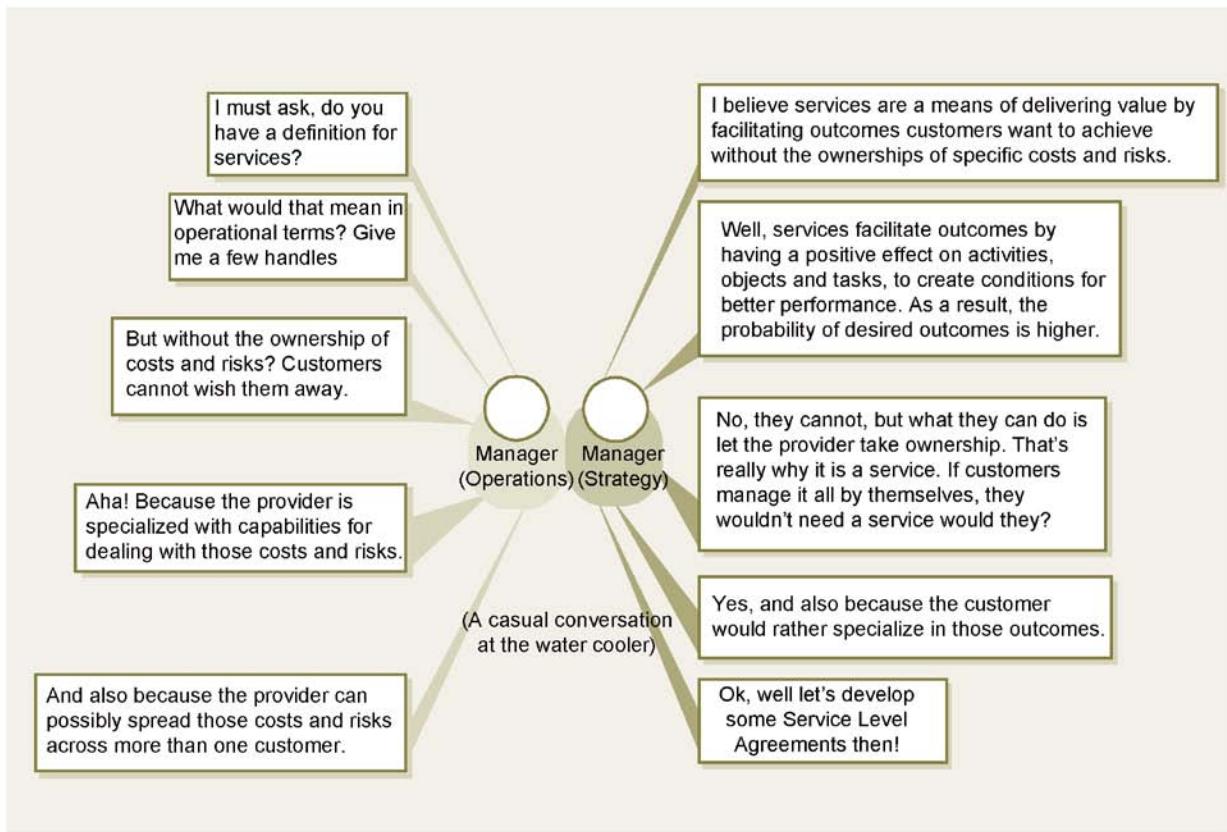


Figure 2.A – The importance of terminology

© Crown Copyright 2007 Reproduced under license from OGC

Terminology	Explanations
IT Service Management:	A set of specialized organizational capabilities for providing value to customers in the form of services.
Capabilities:	The ability of an organization, person, process, application, CI or IT service to carry out an activity. Capabilities can be described as:
	<ul style="list-style-type: none">• The functions and processes utilized to manage services.• Intangible assets of an organization that cannot be purchased, but must be developed and matured over time.
	<p><i>The ITSM set of organizational capabilities aims to enable the effective and efficient delivery of services to customers.</i></p>
Resources:	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.
Process:	A set of <i>coordinated activities</i> combining and implementing resources and capabilities in order to produce an outcome and <i>provide value to customers or stakeholders</i> .
	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.
Service:	A means of delivering value to Customers by facilitating outcomes customers want to achieve without the ownership of specific costs or risks
Functions:	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>
	<ul style="list-style-type: none">• Service Desk• Technical Management• Application Management• IT Operations Management

Terminology	Explanations
Process Owner:	The person responsible for ensuring that the process is fit for the desired purpose and is accountable for the outputs of that process. Example: The owner for the Availability Management Process
Service Owner:	The person who is accountable for the delivery of a specific IT Service. They are responsible for continual improvement and management of change affecting Services under their care. Example: The owner of the Payroll Service
Process Manager:	The person responsible for the operational management of a process. There may be several Managers for the one process. They report to the Process Owner.
Internal Service Providers:	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.
Shared Service Providers:	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 typically don't provide a source of competitive advantage, but instead <i>support effective and efficient business processes</i> .
External Service Providers:	Service provider that provides IT services to external customers i.e. outsourcing
Business Case:	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.

2.1 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, with the focus being the Service oriented or end-to-end view of 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*”. Well what does this actually mean? To explain some of the key concepts I will use an analogy that most (food lovers) will understand.

While I do enjoy cooking, there are often times where I wish to enjoy quality food without the time and effort required to prepare a meal. If I was to cook, I 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 of course, I can go to a restaurant that delivers a service that provides me with the same outcome (a nice meal) without the time, effort and general fuss if I was to cook it myself.

Now consider how I would identify the quality and value of that service being provided. It isn't just the quality of the food itself that will influence my 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 my meal (and was it what I asked for?).
- Did they offer water as well as normal drinks and beverages?

If just one of these factors don't meet my expectations than ultimately the perceived quality and value being delivered to me as a customer are negatively impacted.

Now relate this to our role in providing an IT Service. If we as IT staff focus on the application or hardware elements being 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 we take a Service oriented perspective, we 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.

2.2 Processes & Functions

2.2.1 Defining Processes

Processes can be defined as a structured set of coordinated activities designed to produce an outcome and provide value to customers or stakeholders. A process takes one or more inputs and through the activities performed turns them into defined outputs.

Some principles:

- All processes should be measurable and performance driven (not just time, but measuring overall efficiency including cost, effort and other resources used).
- Processes are *strategic assets* when they create competitive advantage and market differentiation.
- Processes *may* define roles, responsibilities, tools, management controls, policies, standards, guidelines, activities and work instructions if they are needed.

A *process owner* is the person responsible for ensuring that the process is fit for the desired purpose and is accountable for the outputs of that process.

A *process manager* is the person responsible for the operational management of a process. There may be several Managers for the one process or the same person may be both the process owner and process manager (typically in smaller organizations).

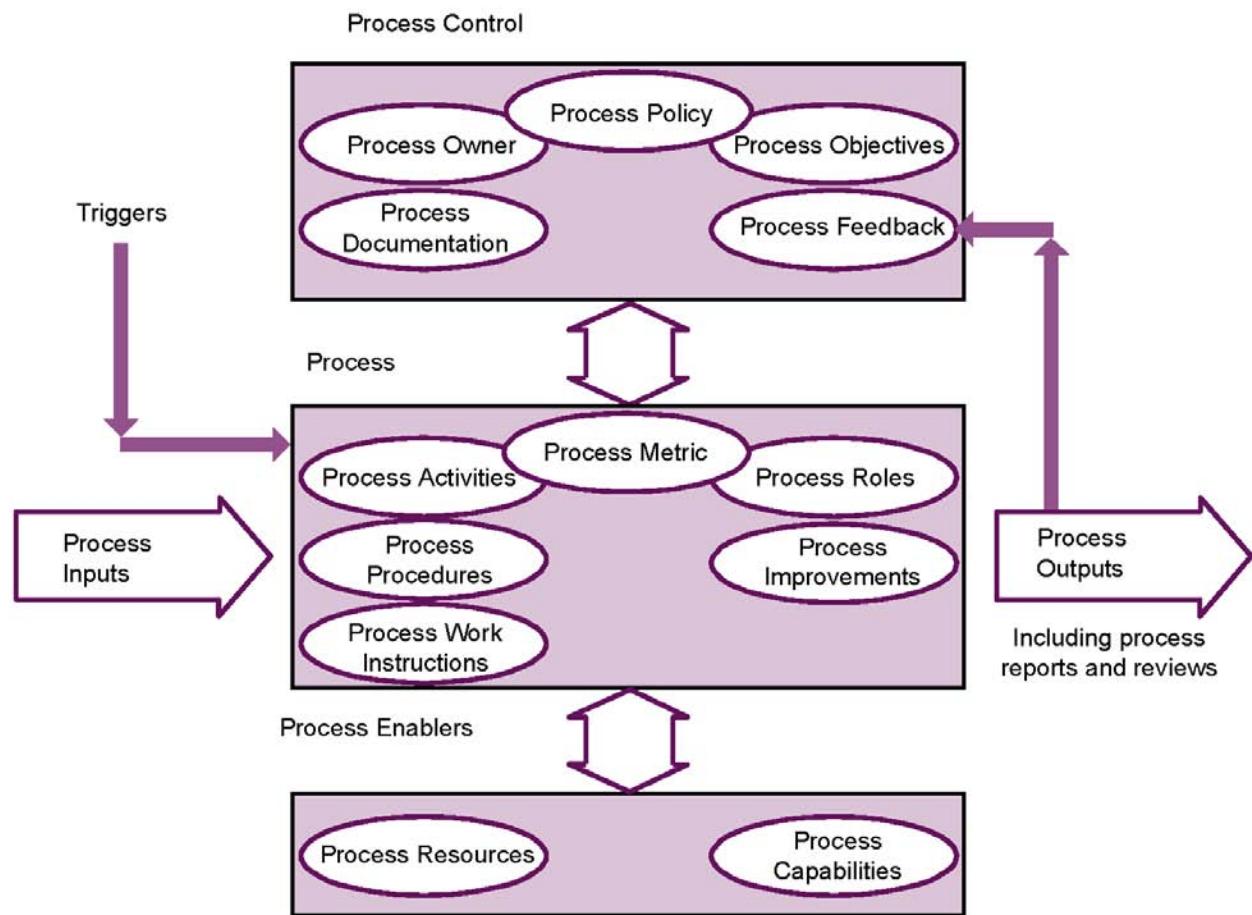


Figure 2.B – Generic Process Elements
 © Crown Copyright 2007 Reproduced under license from OGC

The figure above 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. Behavioural components have no independent existence apart 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 behavioural 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 behaviours 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 to be empowered in the change being developed, and therefore are more likely to respond positively rather than actively or passively resisting the organizational changes occurring.

2.2.2 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 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 design, delivery and management IT Services.

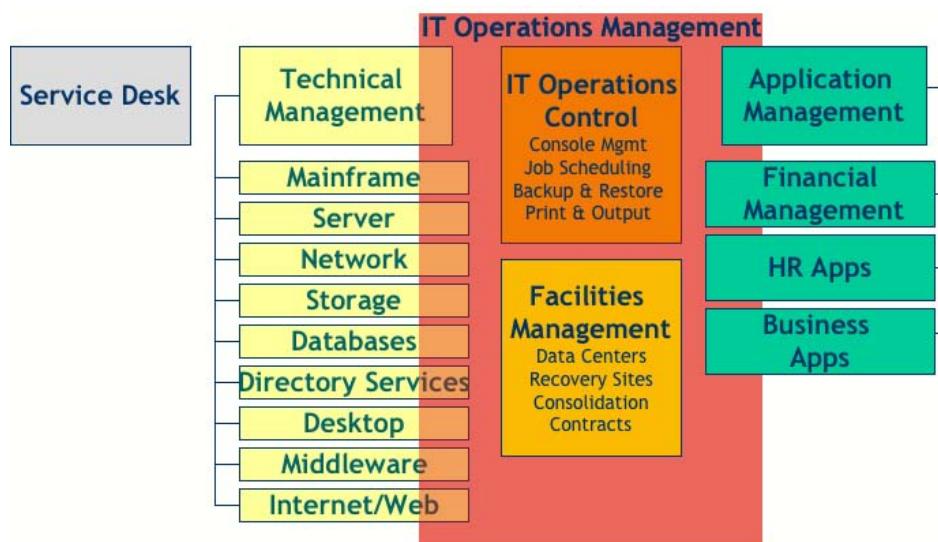


Figure 2.C – The ITIL® Functions from Service Operation

2.2.3 Connecting Processes and Functions

It is often said that processes are perfect... until people get involved. This saying comes from failure when executing processes due to misunderstandings of the people involved and a lack of clarity regarding the roles and responsibilities that exist. A useful tool to assist 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).

RACI Model

	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 (shows that actions are taking place), with more than one being appropriate where there is shared responsibility.

3 The Service Lifecycle

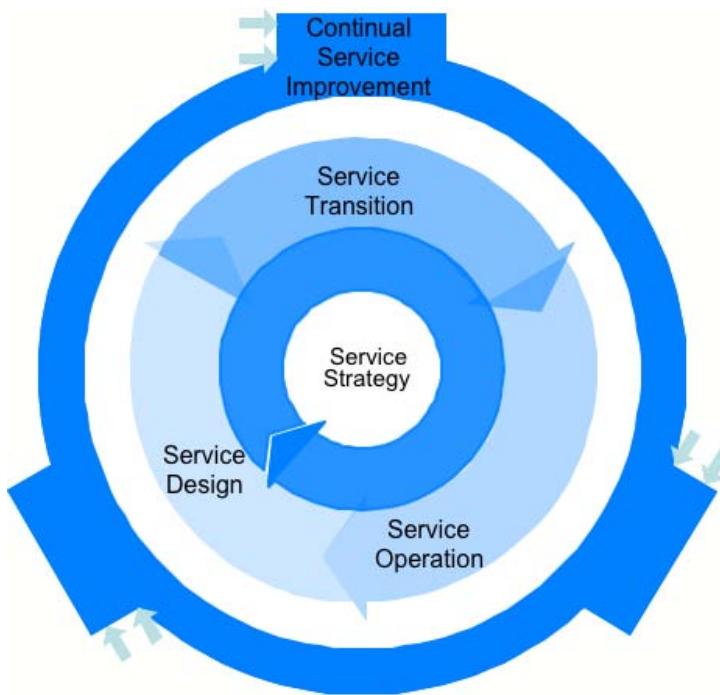


Figure 3.A – ITIL® Service Lifecycle Model
© Crown Copyright 2007 Reproduced under license from OGC

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

The concept of the **Service Lifecycle** is fundamental to the refresh of ITIL® for Version 3. 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 Version 3 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 phases 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 (books).

3.1 Mapping the Concepts of ITIL® to the Service Lifecycle

There has been much debate as to exactly how many processes exist within Version 3 of ITIL®. Questions asked include:

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

In developing this material we have based our definitions of processes and functions and where they fit on the guidance provided by the ITIL® Foundation syllabus by EXIN International. Figure 3.B demonstrates the processes and functions of ITIL® in relation to the 5 Service Lifecycle Phases. It also demonstrates the increased scope now covered by ITIL® over the previous version.

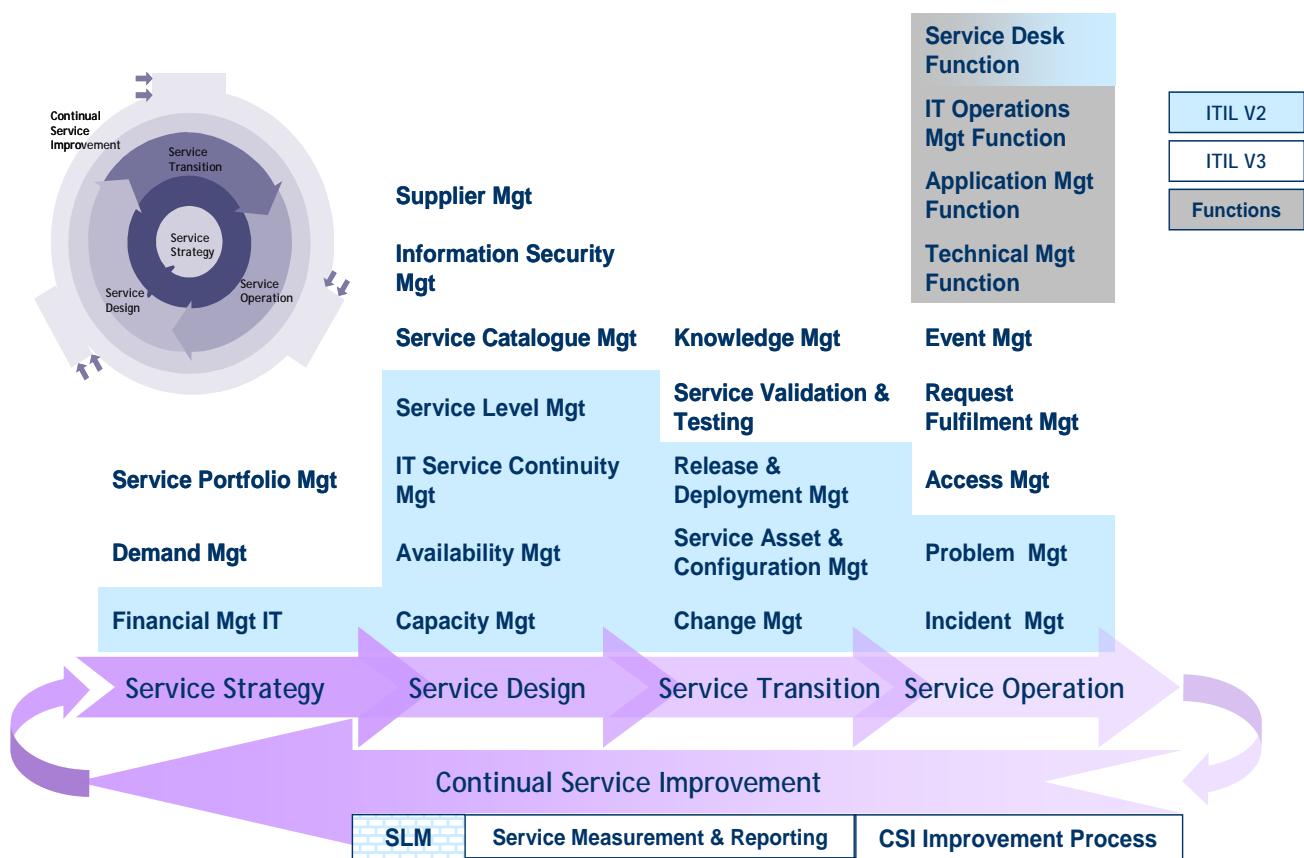


Figure 3.B – The Major Concepts of ITIL®

NOTES:

- The Service Lifecycle phases (and ITIL® books) are shown through the arrows at the bottom;
- The concepts in light shading are the V2 ITIL® concepts;
- The concepts not shaded are the new ITIL® V3 concepts;
- The concepts in dark shading are Functions.

Although Service Level Management officially sits in the Service Design book, it plays a very important role in the Continual Service Improvement phase, and therefore could also fit in the CSI book as a process.

3.2 How does the Service Lifecycle work?

Although there are 5 phases throughout the Lifecycle, they are not separate, nor are the phases necessarily carried out in a particular order. The whole ethos of the Service Lifecycle approach is that each phase will affect the other, creating a continuous cycle. For this to work successfully, the Continuous Service Improvement (CSI) phase is incorporated throughout all of the other phases. Figure 3.C demonstrates some of the key outputs from each of the Service Lifecycle Phases.

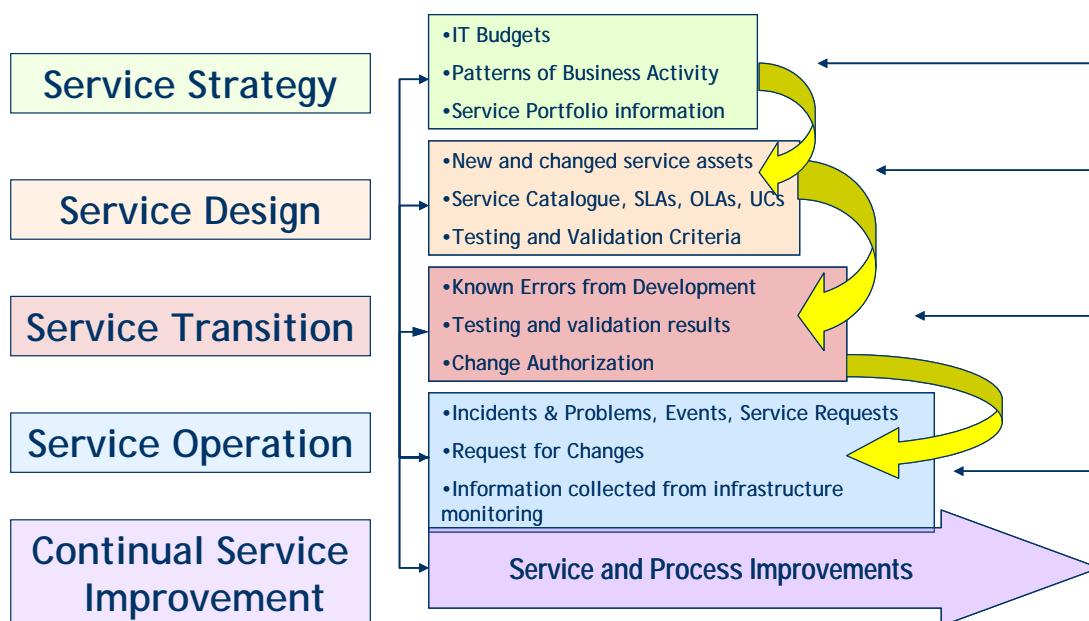
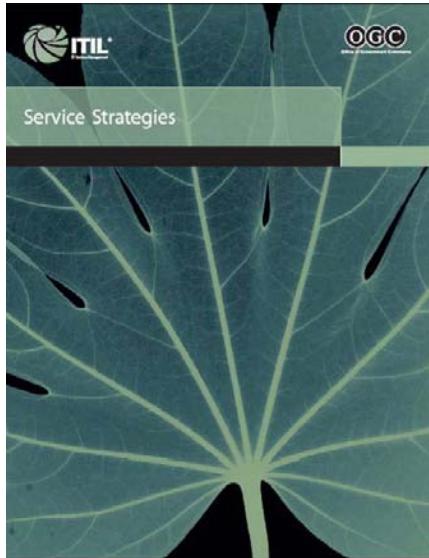


Figure 3.C – How does the Service Lifecycle Work?

It is important to note that most of the processes defined do not get executed within only one lifecycle phase. As an example:

- **Service Strategy Phase:** Determine the needs, priorities, demands and relative importance for desired services. Identifies the value being created through services and the predicted financial resources required to design, deliver and support them.
- **Service Design Phase:** Designs the infrastructure, processes and support mechanisms needed to meet the Availability requirements of the customer.
- **Service Transition Phase:** Validates that the Service meets the functional and technical fitness criteria to justify release to the customer.
- **Service Operation Phase:** Monitors the ongoing Availability being provided. During this phase we also manage and resolve incidents that affect Service Availability.
- **Continual Service Improvement Phase:** 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.

4 Service Strategy



The Service Strategy phase 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.
- Strategy and Service Economics.
- How strategy affects the Service Lifecycle.
- Strategy and organizational culture and design.

Figure 4.A: Service Strategy

4.1 Objectives

The primary objectives of Service Strategy are to:

- Design, develop and implement service management as a strategic asset and assisting growth of the organization.
- Develop the IT organization's capability to manage the costs and risks associated with their service portfolios.
- Define the strategic objectives of the IT organization.

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

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

4.2 Major Concepts

4.2.1 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 apple 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 support this need, one of the major elements of the Service Strategy lifecycle is the creation of value through Services and Service Packages.

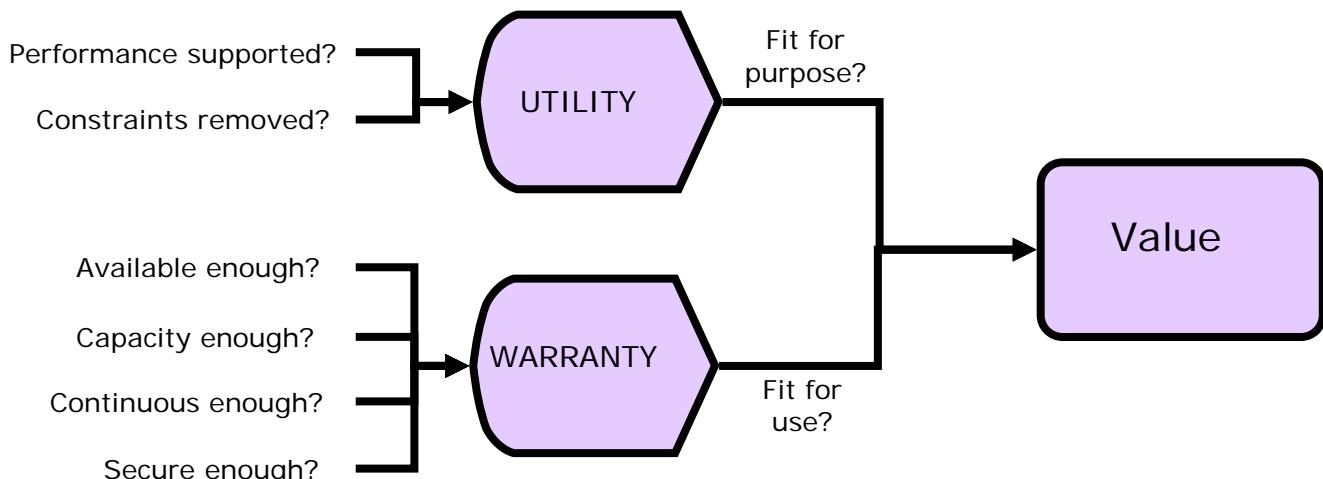


Figure 4.B – Creating Service Value
© Crown Copyright 2007 Reproduced under license from OGC

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.

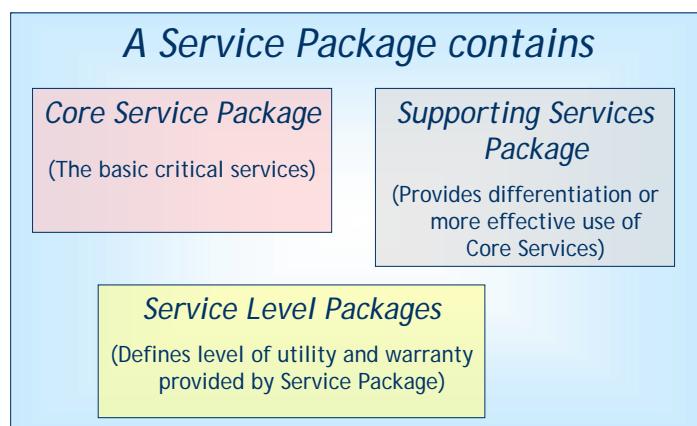
Service Warranty on the other hand describes how well these benefits are delivered to the customer. It describes the Service's attributes such as the availability, capacity, performance, security and continuity levels to be delivered by the provider. Importantly, the Service Utility potential is only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

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.

4.2.2 Service Packages and Service Level Packages

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

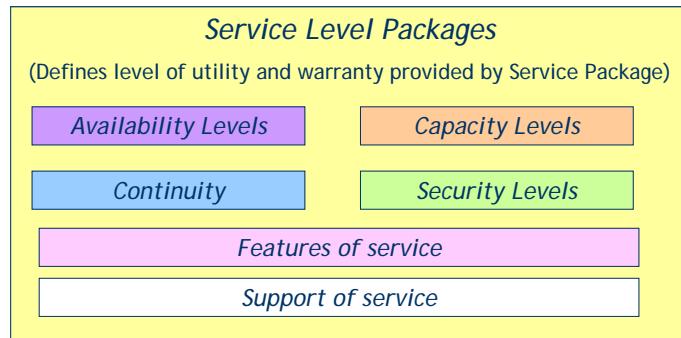
As customers, we have a wide range of choice when looking for an ISP to provide broadband internet. So as a result ISPs do need to work hard to attract customers by communicating the value that they provide through their offerings. They also need to offer a wide range of choice for customers, who have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



A **Service Package** provides a detailed description of 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 (often the excitement factors)
- The Service Level Package (see next page)

Figure 4.C – Service 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 & Capacity Levels
- Continuity Measures
- Security Levels

Figure 4.D – Service Level Package Example

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

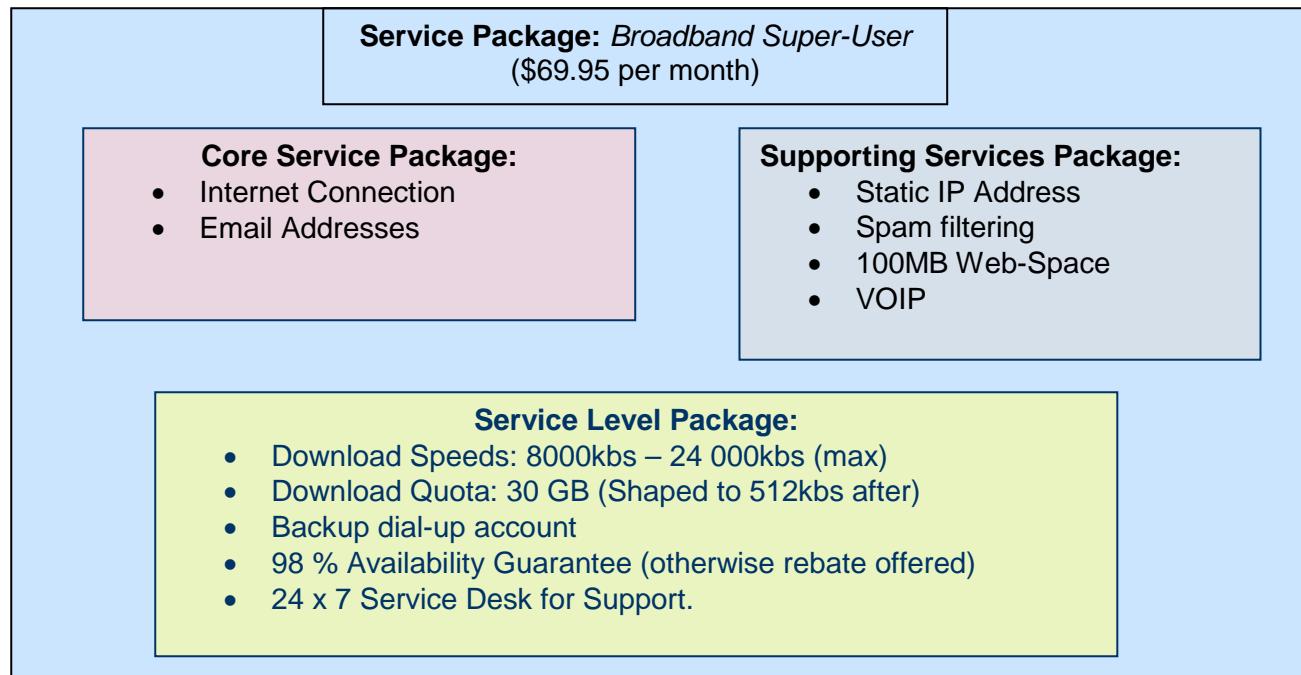


Figure 4.E – Detailed Service Package Example (ISP)

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.

4.3 Service Strategy Processes

The processes included in the Service Strategy lifecycle phase are:

- Service Portfolio Management
- Financial Management
- Demand Management

These three processes work together to enable an IT organization to maximize the value of services being provided to customers and to provide the quality information required to make investment decisions regarding IT.

4.3.1 Service Portfolio Management

Goals and Objectives:

The primary goal of Service Portfolio Management is to provide strategic direction and management of investments into IT Service Management so that an optimum portfolio of services is continually maintained.

Other objectives include:

- To provide an improved ability for supporting and enhancing business processes and business services.
- To identify and define the business value provided by IT services.
- To maintain accurate information regarding planned, current and retired IT services.

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 risk?
- How are resources and capabilities to be allocated?

Scope:

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.

Services are grouped into three distinct categories in the Service Portfolio:

- Service Pipeline (services that have been proposed or in development).
- Service Catalogue (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 Catalogue 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.

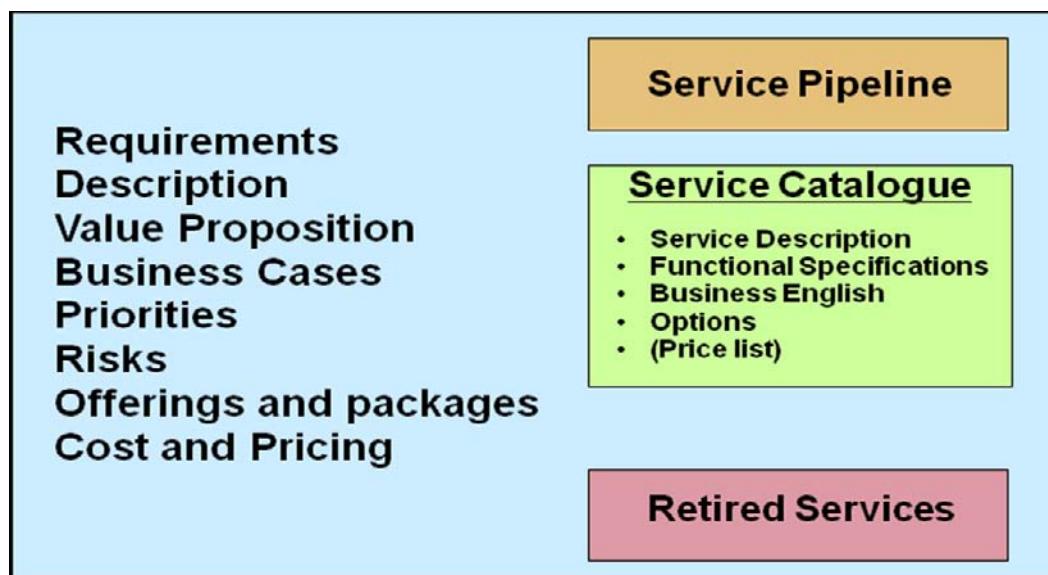


Figure 4.F – A Service Portfolio

Service Portfolio Management is a dynamic and ongoing process and includes the following methods:

Define: Used to validate portfolio data. It is the assessment of services investment in terms of potential benefits and the resources and capabilities required to provision and maintain them. This also enables the Service Provider to define what it cannot do (due to maturity levels, capabilities, risks etc). Through this activity, the initial creation of the Service Portfolio begins.

Analyze: Maximize portfolio value, align, prioritize and balance supply and demand. This is where strategic intent is created. Questions asked here include:

- What are the long term goals of the service organization?
- What services are required to meet those goals?
- What capabilities and resources are required to deliver and support those services?
- How will we get there?

Approve: Finalize proposed portfolio; authorize services and resources needed to deliver services.

Charter: Plans and tracks the progress of service investments across the portfolio and allocate the required resources. Used to schedule and manage the design, transition, change and retirement of services.

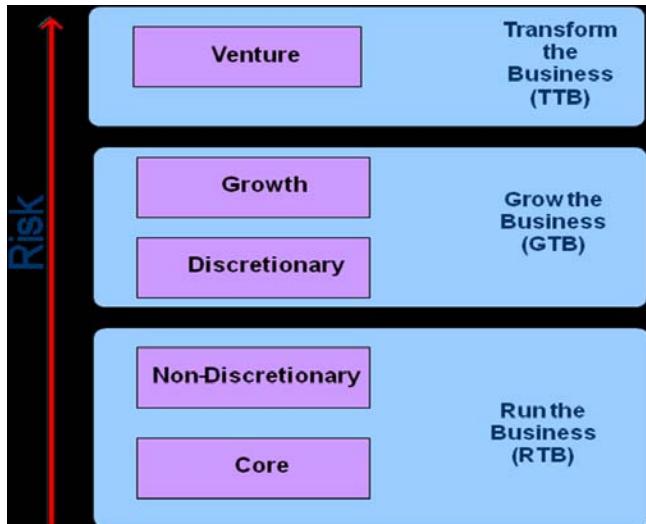


Figure 4.G – Balancing a Service Portfolio

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

Investment Categories & 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.

Run the Business (RTB):

RTB investments are centered on maintaining service operations

Figure 4.H – Balancing a Service Portfolio

The outcomes for existing services fall into 6 categories:

- RENEW:** These services meet functional fitness criteria, but fail technical fitness.
- REPLACE:** These services have unclear and overlapping business functionality.
- RETAIN:** Largely self contained, with well defined asset, process and system boundaries. These services are aligned with and are relevant to the organization's strategy
- REFACTOR:** Often services that meet the technical and functional criteria of the organization display fuzzy process or system boundaries. In these cases, the service can often be refactored to include only the core functionality, with common services used to provide the remainder.
- RETIRE:** Retired services that do not meet minimum levels of technical and functional fitness.
- RATIONALIZE:** Used to address portfolios that offer services which in fact are composed of multiple releases of the same operating system, service or application etc.

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

While the previous section discussed the methods of Service Portfolio Management in an ordered fashion, in reality these methods form part of a continuous cycle that seeks to refresh the Service Portfolio, making 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 & low reward, high risk & potential high reward) and authorize service investments that match these needs.

4.3.2 Financial Management

GOAL: The goal of Financial Management is to provide cost effective stewardship of the IT assets and the financial resources used in providing IT services. Primarily this is to enable an organization to account fully for the financial resources consumed by the IT service provider and to attribute these costs to the services delivered to the organization's customers.

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.

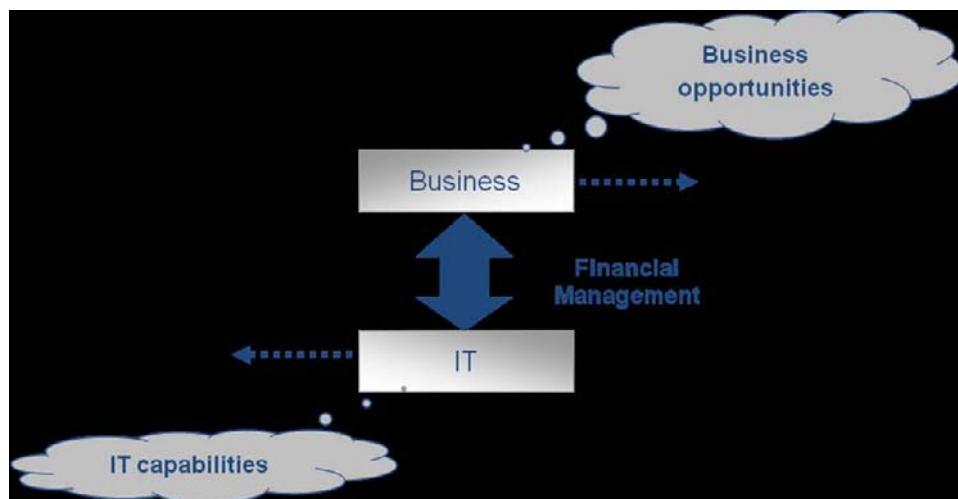


Figure 4.I – Financial Management managing conflicting perspectives

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.

Activities

There are three fundamental activities for Financial Management for IT Services. These are:

1. Funding
 2. IT Accounting
 3. Chargeback
-
1. **Funding:** 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.
 2. **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.
 3. **Chargeback (optional activity):** 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

(Not examined at a Foundation level)

Terminology	Explanations
Cost Types:	These are higher level expenses identified such as hardware, software, people, accommodation, transfer and external costs.
Cost Elements:	The actual elements making up the cost types above e.g. for the hardware cost type it would include the elements such as CPUs, Servers, Desktops etc.
Direct Costs:	Cost elements identified to be clearly attributed to only a single customer or service.
Indirect Costs:	Often known as overheads, these are costs that are shared across multiple customers or services, which have to be shared in a fair manner.
Cost Units:	A cost unit is the identified unit of consumption that is accounted for a particular service or service asset.

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 in chapter 4.2, value in services is created by the combination of Service Utility and Service Warranty.

Demand Modelling:

Financial Management works closely with the process of Demand Management (see Chapter 4.3.3) to anticipate usage of services by the business and the associated financial implications of future service demand. This assists in identifying the funding requirements for services, as well as input into proposed pricing models, including any incentives and penalties used.

Strategically, financial input can be gained from key times such as product launches, entry into new markets, mergers and acquisitions, which all generate specific patterns of demand. From a customer perspective, the Service Catalogue should provide the capability to regulate their demands for IT services and prepare budgets, avoiding the problem of over-consumption.

4.3.3 Demand Management

GOAL: The primary goal of Demand Management is to assist the IT Service Provider in understanding and influencing Customer demand for services and the provision of Capacity to meet these demands.

Other objectives include:

- Identification and analysis of Patterns of Business Activity (PBA) and user profiles that generate demand.
- Utilizing techniques to influence and manage demand in such a way that excess capacity is reduced but the business and customer requirements are still satisfied.

Demand Management was previously an activity found within Capacity Management, and now within Version 3 of ITIL® it has been made a separate process found within the Service Strategy phase. The reasoning behind this is that before we decide how to design for capacity, decisions must be made regarding why demand should be managed in a particular way. Such questions asked here include:

- When and why does the business need this capacity?
- Does the benefit of providing the required capacity outweigh the costs?
- Why should the demand for services be managed to align with the IT strategic objectives?

Keep in mind that Demand Management plays an integral part in supporting the objectives of an organization and maximizing the value of the IT Service Provider. This means that the way in which Demand Management is utilized will vary greatly between each organization. Two examples showing these differences are:

- **Health Organizations:** When providing IT Services that support critical services being offered to the public, it would be unlikely that there would be many (if any) demand management restrictions that would be utilized, as the impact of these restrictions could lead to tragic implications for patients being treated.
- **Commercial Confectionery Organizations:** Typically a confectionery company will have extremely busy periods around traditional holidays (e.g. Christmas). Demand Management techniques would be utilized to promote more cost-effective use of IT during the non-peak periods; however leading up to these.

Activity-based Demand Management

The primary source of demand for IT services comes from the execution of business process within the organization(s) being served. With any business process, there will be a number of variations in workload that will occur, which are identified as patterns of business activity (PBA) so that their affect on demand patterns can be understood. By understanding exactly how the customer's business activity operates, the IT organization can improve the way in which capacity is planned and produced for any supporting services.

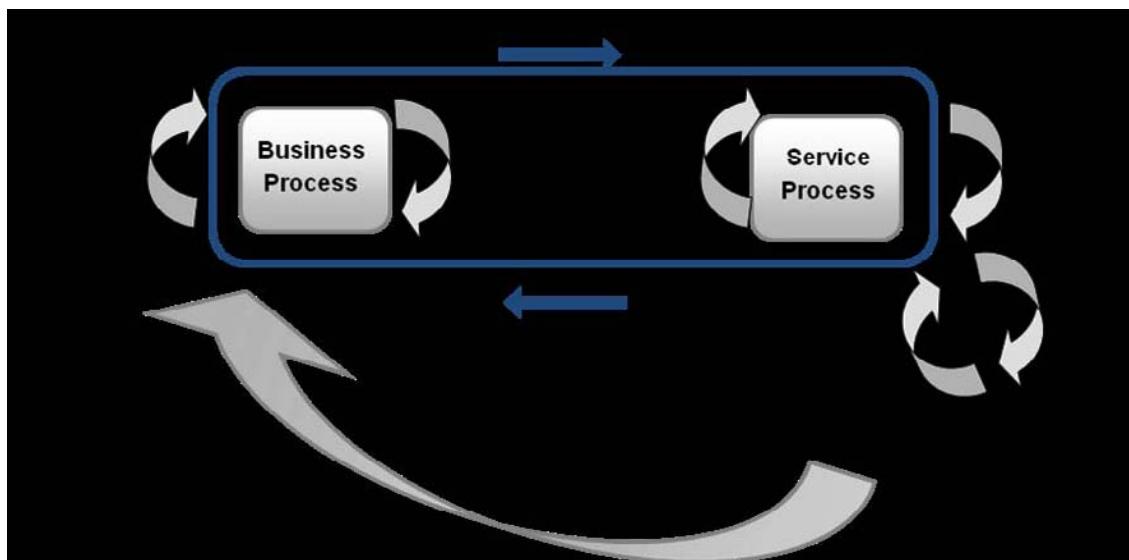


Figure 4.J: – Activity-based Demand Management
© Crown Copyright 2007 Reproduced under license from OGC

Over time, Demand Management should be able to build a profile of business processes and the patterns of business activity in such a way that seasonal variations as well as specific events (e.g. adding new employees) can be anticipated in terms of associated demand. Using this information will help various elements of the Service Lifecycle, including the following:

- **Service Design:** Particularly Capacity and Availability Management, who can optimize designs to suit demand patterns.
- **Service Transition:** Change Management and Service Validation and Testing can ensure that appropriate levels of warranty can be provided.
- **Service Operation:** Can optimize the availability of staff based on patterns of demand.
- **Continual Service Improvement:** Can identify opportunities to consolidate demand or introduce improved incentives or techniques to be utilized in influencing demand.

There are two ways to influence or manage demand:

1. Physical/Technical constraints e.g. restrict number of connections, users, running times
2. Financial chargeback e.g. using expensive charging for services near full capacity or over capacity quotas

Demand Management needs to work closely with the other Service Strategy processes (Financial Management & Service Portfolio Management), as well as Service Level Management in ensuring the appropriate development of Service Packages that positively influence the demand and consumption of IT resources and services.



Figure 4.K – Using Demand Management to Optimize IT Capacity

QUESTION: Every morning between 8:00am and 8:30am, approximately 1500 users logon to the network. At the same time, many IT services, batch jobs and reports are run by various groups throughout the organization.

Recently the performance of the IT infrastructure has been experiencing problems during this time period (e.g. taking a long time to log on, reports and batch jobs failing) Outside of this time, the IT infrastructure performs at acceptable levels.

What are some Demand Management techniques that could be utilized to address this situation?

- Staggering work start times
- Prioritizing reports and batch jobs
- Running non-time-critical reports and batch jobs at night or outside typical work hours
- Restricting any non-critical activities during peak periods

4.4 Service Strategy Summary

The Service Strategy phase 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:

4.4.1 Interfaces with the Service Design Phase

- 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.

4.4.2 Interfaces with the Service Transition Phase

- 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 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.

4.4.3 Interfaces with the Service Operation Phase

- Service Operation will deploy service assets in patterns that most effectively deliver the required utility and warranty in each segment across the Service Catalogue.
- 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.

4.4.4 Interfaces with the Continual Service Improvement Phase

- 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.

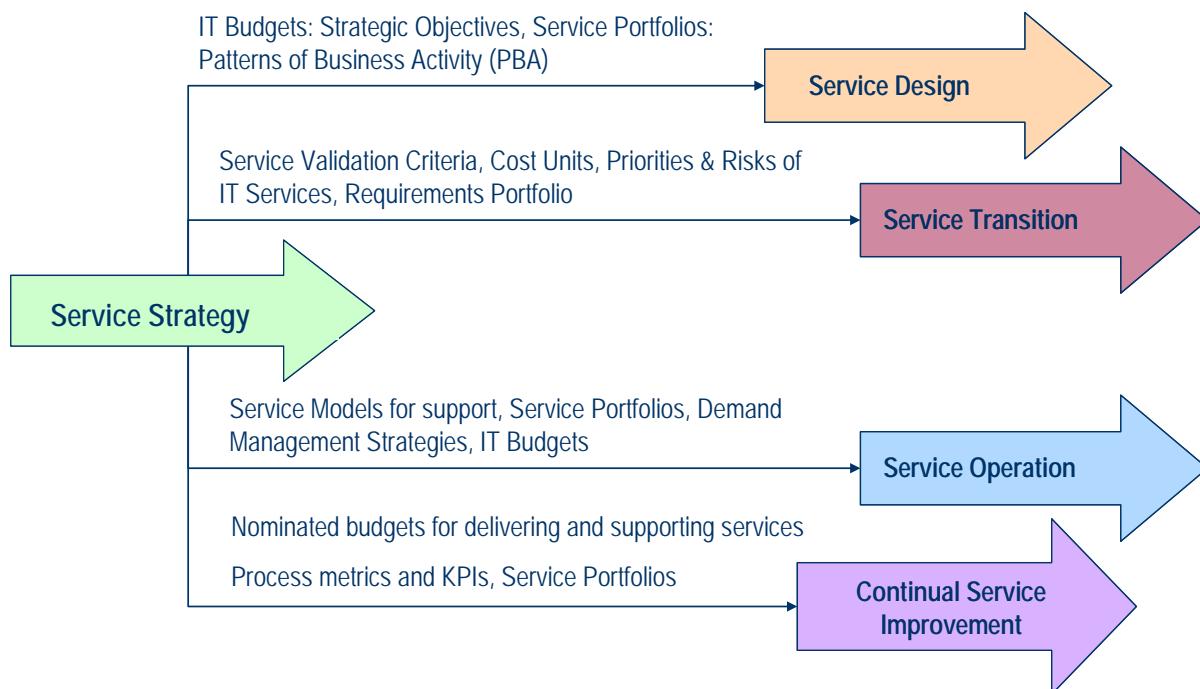


Figure 4.L – Some Service Strategy outputs to other lifecycle phases.

4.5 Service Strategy Service Scenario

To assist with your learning and understanding of how the phases 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 shall call this new service HYPE!

4.5.1 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

4.5.2 Service Portfolio Management Considerations

- You have already been trialing X brand instant messenger service among the IT staff, so it is in your pipeline
- Can we produce it, or do we need to buy it?
- Service Catalogue – nil
- What gap is it filling in the portfolio?
- Are there redundant services to retire?

4.5.3 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?

4.5.4 Demand Management Considerations

- When would business most need service? (mornings and afternoons, as they are most likely to interact with international counterparts - time zones), times of year?
- What measures can we take to manage demand?
 - Limit VOIP/video to certain groups/users
 - Charge business for use
 - Dedicated bandwidth across whole of service

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 value of HYPE is seen. As we all know, the level of value will more than likely be in direct correlation to the \$\$ the business is prepared to pay, and this is why it is important to clarify this now, before we start designing.

4.6 Service Strategy Review Questions

These questions also cover the Introduction and Common Terminology Chapters.

4.6.1 Question 1

Which ITIL® process is responsible for drawing up a charging system?

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

4.6.2 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

4.6.3 Question 3

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

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

4.6.4 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

4.6.5 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

4.6.6 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

4.6.7 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

4.6.8 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

4.6.9 Question 9

The 4 P's of ITSM are people, partners, processes and:

- a) Purpose
- b) Products
- c) Perspectives
- d) Practice

4.6.10 Question 10

The contents of a service package include:

- 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 Packages

5 Service Design



Figure 5.A – Service Design

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

- Processes.
- Service Management systems and tools.
- Service Solutions.
- Technology architectures.
- Measurement systems.

The driving factor in the design of new or changed services is to support 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.

5.1 Objectives

While there are many elements within the Service Design phase, the three main objectives that provide direction to the processes involved are:

- To convert the strategic objectives defined during Service Strategy into Services and Service Portfolios.
- To use a holistic approach for design to ensure integrated end-to-end business related functionality and quality.
- To ensure consistent design standards and conventions are followed in all services and processes being designed.

5.2 Major Concepts

5.2.1 Five Major Aspects of Service Design

An overall, integrated approach should be adopted for the design activities, covering five major aspects of Service Design:

1. **Service Portfolio:** Service Management systems and tools, especially the Service Portfolio for the management and control of services through their lifecycle.
2. **Service Solutions:** including all of the functional requirements, resources and capabilities needed and agreed.
3. **Technology architectures:** Technology architectures and management architectures and tools required to provide the service.
4. **Processes:** Processes needed to design, transition, operate and improve the service.
5. **Measurement systems:** Measurement systems, methods and metrics for the services, the architectures and their constituent components and the processes.

The key aspect in the design of new or changed services is to meet changing business needs. Every time a new service solution is produced, it needs to be checked against each of the other aspects to ensure that it will integrate and interface with all of the other services in existence.

5.2.2 Service Design Packages

The information contained within a Service Design Package including all aspects of the service and its requirements is used to provide guidance and structure through all of the subsequent stages of its lifecycle. A Service Design Package is 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 & Topology
- Organizational Readiness Assessment
- User Acceptance Test Criteria
- Service Program
- Service Transition Plan
- Service Operational Plan
- Service Acceptance Criteria

5.3 Service Design Processes

The processes included with the Service Design lifecycle phase are:

- Service Level Management (Design)
- Capacity Management
- Availability Management
- IT Service Continuity Management
- Information Security Management
- Supplier Management
- Service Catalogue Management

It is important to note that many of the activities from these processes will occur in other lifecycle phases, 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 actual SOA team may be a single person in a small IT department or involve a worldwide network of business and customer oriented groups in an international organization.

5.3.1 Service Level Management

GOAL: The primary goal of Service Level Management is to ensure that an agreed level of IT service is provided for all current IT services, and that future services are delivered to agreed achievable targets. It also proactively seeks and implements improvements to the level of service delivered to customers and users.

By acting as the liaison between the IT Service Provider and the customers, Service Level Management (SLM) is utilized to ensure that the actions required for gathering requirements, developing agreements, and measuring and reporting performance are performed in a consistent manner in line with the needs of the business and customers.

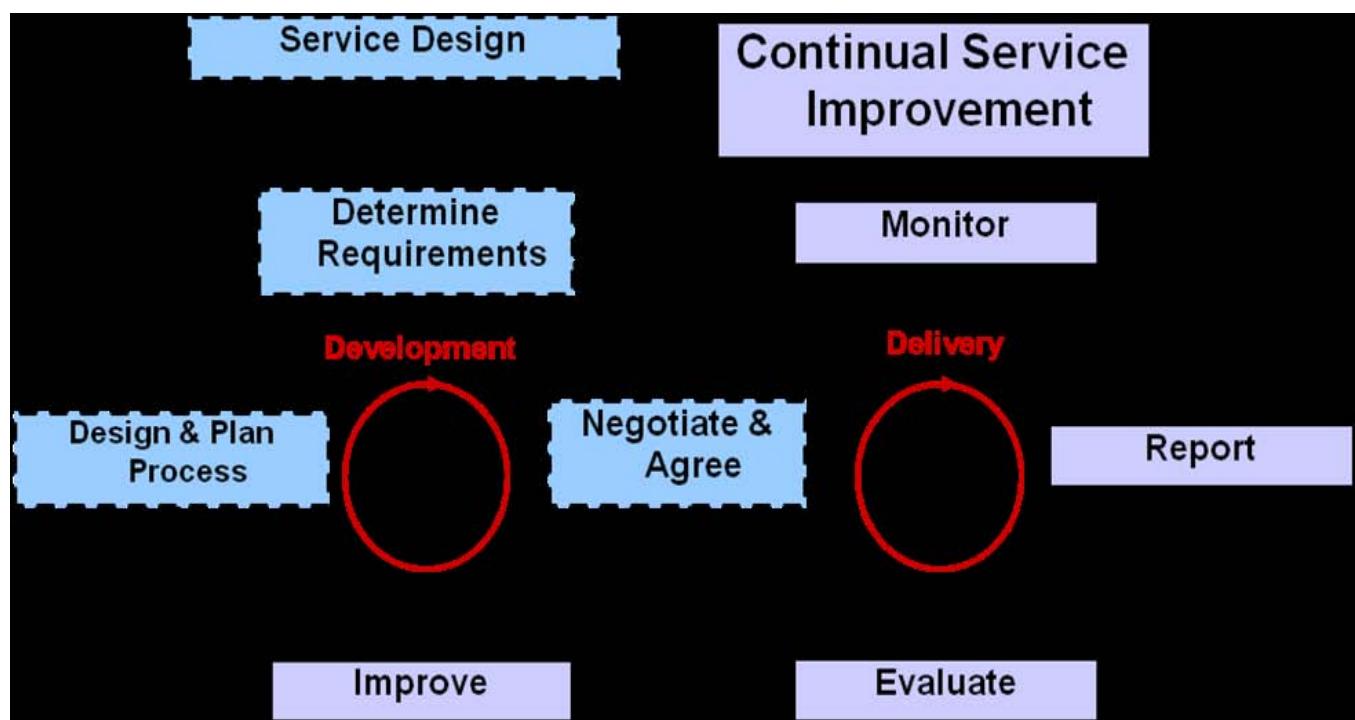


Figure 5.B – The Activities of Service Level Management

During the Service Design lifecycle phase, Service Level Management:

- Designs and plans the SLM process and Service Level Agreement (SLA) Structure;
- Determines the Service Level Requirements (SLRs);
- Negotiates and Agrees upon the relevant Service Level targets with customers to produce SLAs;
- Negotiates and agrees upon the support elements required by the internal IT groups and External Suppliers to produce Operational Level Agreements (internal) and Underpinning Contracts (external).

Terminology	Explanation
Service Level Agreement (SLA):	A written agreement between a service provider and their Customers that documents agreed levels of service for a Service.
Service Catalogue:	A written statement of available IT services, default levels, options, prices and identification of which business processes or customers use them.
Underpinning Contract (UC):	Contract with an external supplier that supports the IT organization in their delivery of services.
Operational Level Agreement (OLA):	Internal agreement with another area of the same organization which supports the IT service provider in their delivery of services.
Service Level Requirements:	Detailed recording of the Customer's needs, forming the design criteria for a new or modified service.

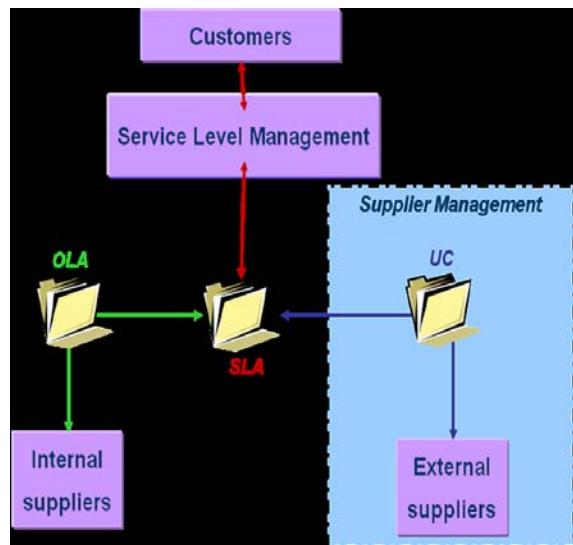


Figure 5.C – SLAs, OLAs and UCs

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.

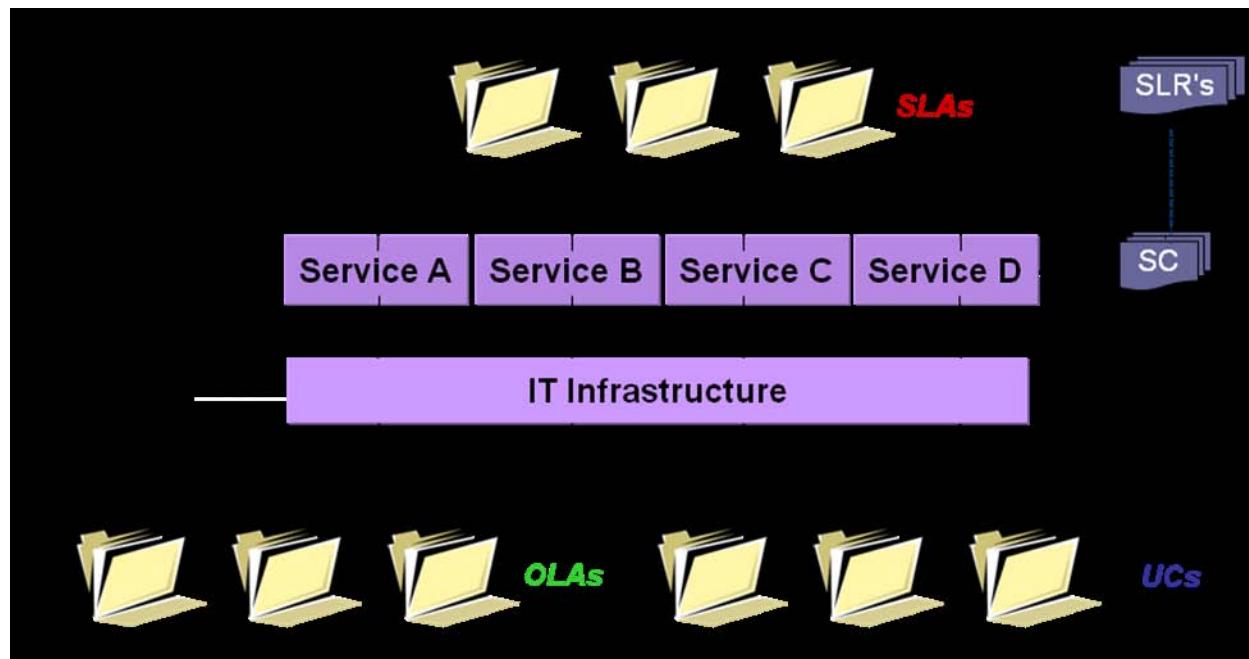


Figure 5.D – How SLAs, OLAs and UCs fit together

QUESTION: According to the ITIL® framework which of these documents should be developed first in an organization that is already delivering services?

ANSWER: The Service Catalogue: because we need to define what we are providing first, and then we can map the customer requirements to the Service Catalogue to see what gaps or redundant service exist.

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, in that SLAs should not be used as a way of holding one side or the other to ransom. When SLAs are viewed in a positive nature as a way of continually improving the relationship between provider and customers, mutual beneficial agreements will be developed, rather than the development of contracts as part of a 'blame culture' by both parties.

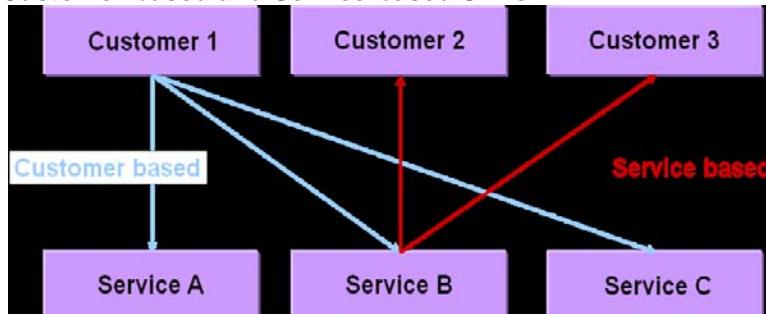
Service Level Agreement Structures

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 SLAs structures that are discussed within ITIL® are Service-based, Customer-based and Multi-level or Hierarchical SLAs.

Customer-based and Service-based SLAs



Multi-level SLAs

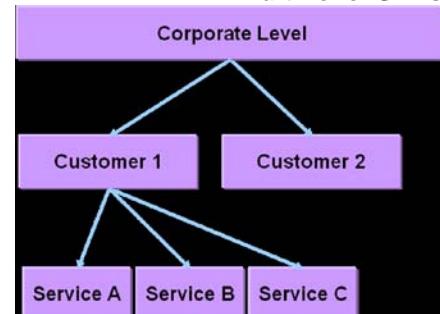


Figure 5.F – SLA structures

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 needs 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 & 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 measureable, 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 they that become too long and technically focused. When this occurs there is potential for misunderstandings or even for the SLA to go unread.

See the Continual Service Improvement Chapter for the aspects of Service Level Management that focus on improving the level of quality being delivered for IT Services.

5.3.2 Supplier Management

GOAL: The primary goal of Supplier Management is to manage suppliers and the services they supply, to provide seamless quality of IT service to the business and ensure that value for money is obtained.

Other objectives include the application of capabilities to:

- Obtain value for money from supplier and contracts.
- Ensure that underpinning contracts and agreements with suppliers are aligned to business needs.
- Manage relationships with suppliers.
- Negotiate and agree contracts with suppliers.
- Manage supplier performance.
- Maintain a supplier policy and a supporting Supplier and Contract Database (SCD).

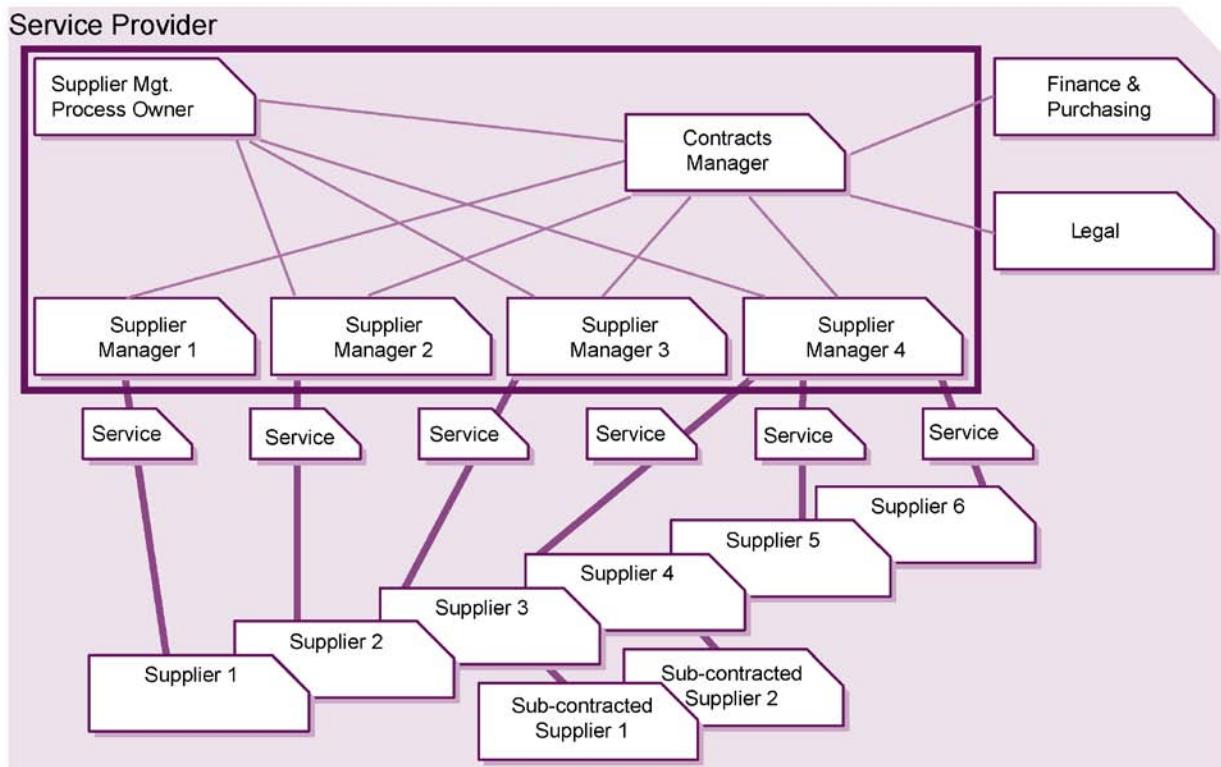


Figure 5.G: – Roles and interfaces for Supplier Management
© Crown Copyright 2007 Reproduced under license from OGC

Terminology	Explanation
Supplier service improvement plans (SSIP):	Used to record all improvement actions and plans agreed between suppliers and service providers.
Supplier Survey Reports:	Feedback gathered from all individuals that deal directly with suppliers throughout their day to day role. Results are collated and reviewed by Supplier Management, to ensure consistency in quality of service provided by suppliers in all areas.
Supplier & Contract performance reports:	Used as input for the Supplier & Contract review meetings to manage the quality of the service provided by suppliers and partners. This should include information on shared risk, when appropriate.

Types of Supplier Arrangements:

Co-sourcing:	An informal combination of insourcing and outsourcing, using a number of outsourcing organizations working together to co-source key elements within the lifecycle.
Partnership or multi-sourcing:	Formal arrangements between two or more organizations to work together to design, develop transition, maintain, operate, and/or support IT service(s). The focus here tends to be on strategic partnerships that leverage critical expertise or market opportunities.
Business Process Outsourcing:	Formal arrangements where an external organization provides and manages the other organization's entire business process(es) or function(s) in a low cost location. Common examples are accounting, payroll and call centre operations.
Knowledge Process Outsourcing:	This is a new enhancement of Business Process Outsourcing, where external organizations provide domain based processes and business expertise rather than just process expertise and requires advanced analytical and specialized skills from the outsourcing organization.
Application Service Provision:	Where external organizations provide shared computer based services to customer organizations over a network. The complexities and costs of such shared software can be reduced and provided to organizations that could otherwise not justify the investment.

Supplier and Contact Database (SCD):

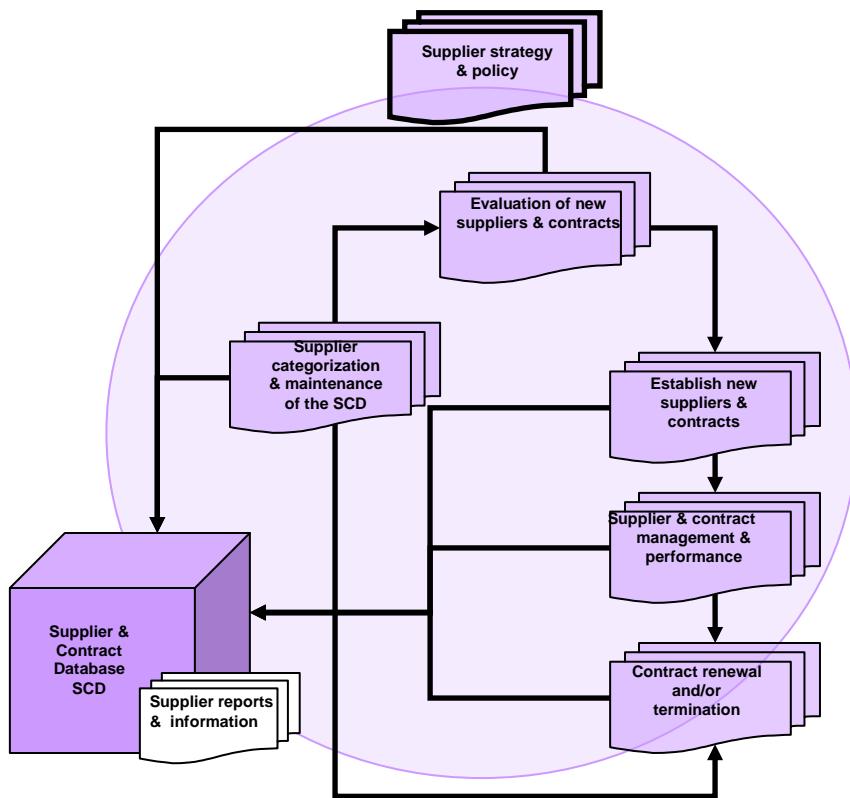


Figure 5.H – The Supplier & Contract Database

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 Database (SCD) should be established.

Ideally the SCD 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 Catalogue.

Relationships with other Lifecycle Phases:

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 Phase	Activities
Service Design	<ul style="list-style-type: none">• Supplier categorization and maintenance of the SCD• Evaluation and set-up of new suppliers and contracts
Service Design	<ul style="list-style-type: none">• Assessing the transition to new suppliers• Establishing new suppliers
Service Operation	<ul style="list-style-type: none">• Supplier and Contract Management and performance• Contract renewal and termination
Continual Service Improvement	<ul style="list-style-type: none">• Identifying improvement actions involving suppliers.• Collating measurements gather on supplier arrangements.

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

5.3.3 Service Catalogue 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 Catalogue 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 become all the more difficult, and things only get worse as time progresses.

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

GOAL: The primary goal of Service Catalogue Management is to ensure that a Service Catalogue is produced, maintained and always contains accurate information on all operational services and those ready for deployment.

Other objectives include:

- To provide a single source of consistent information for communicating available services and their associated details, interfaces and dependencies.
- To ensure that it is widely available to those who are approved to access it.
- To enable mechanisms of self help utilizing technology within the Service Catalogue.

SCOPE: The scope of this process is to provide and maintain accurate information on all services that are being transitioned or have been transitioned to the live environment. This includes such tasks as:

- Definition of the service (what is being provided?).
- Production and maintenance of accurate Service Catalogue information.
- Development and maintenance of the interfaces and dependencies between the Service Catalogue and Service Portfolio, ensuring consistency between the two items.
- Identification and documentation of the interfaces and dependencies between all services (and supporting services) within the Service Catalogue and Configuration Management System (CMS).
- Identification and documentation of the interfaces and dependencies between all services, supporting components and Configuration Items (CIs) within the Service Catalogue and the CMS.

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 Catalogue is logically divided into two aspects:

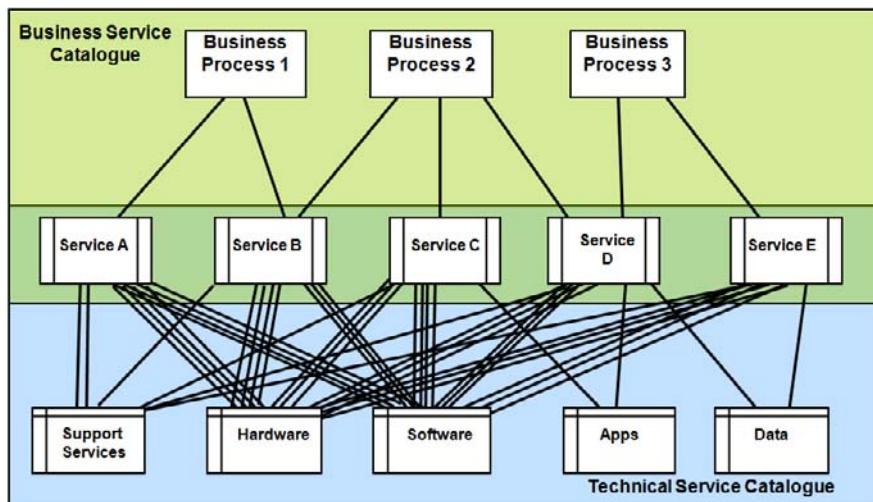


Figure 5.I: – The Business and Technical Service Catalogues

© Crown Copyright 2007 Reproduced under license from OGC

1. A Business Service Catalogue

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 Catalogue, 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 then the technical level of detail provided should be appropriately expanded.

2. A Technical Service Catalogue

Also contains details of all the IT services delivered to the customer, but by comparison, the Technical Service Catalogue 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 Catalogue should underpin the Business Service Catalogue, and is not always be visible to customers and users, unless specifically requested. In many cases the Technical Service Catalogue itself is formed largely by the information contained within the Configuration Management System.

While more extravagant implementations of the Service Catalogue 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.

5.3.4 Capacity Management

GOAL: To ensure the current and future capacity and performance demands of the customer regarding IT service provision are delivered for in a cost-effective manner.

Capacity Management is the process that manages:

- the right capacity,
- at the right location,
- at the right moment,
- for the right customer,
- against the right costs.

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.

- **Too many resources & capabilities**
= *Increased* \$\$\$\$
- **Too little resources & capabilities**
=
decreased performance

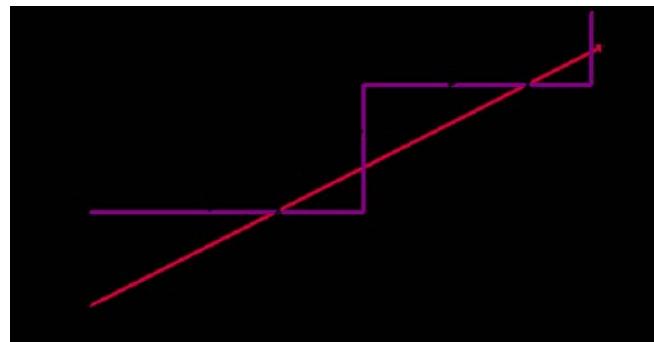


Figure 5.J - The Consequences of Reactive Behaviour

This graph represents the consequences of reactive behavior in managing capacity. The diagonal solid line represents the typical capacity needs of an organization over time. The dotted line represents the Ideal management of capacity to meet the organization's needs. The Horizontal lines depict the reactive approach, whereby investments are put into resolving capacity issues, only when it becomes an issue. This goes well until the next major incident, and more reactive investments are injected to try and "fix" the capacity issues, rather than addressing the issue in a proactive manner.

Sub-Processes of Capacity Management:

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.

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
- Balances loads across resources for optimal performance of services.

All three sub-processes collate their data and report to Service Level Management and Financial Management.

Activities:

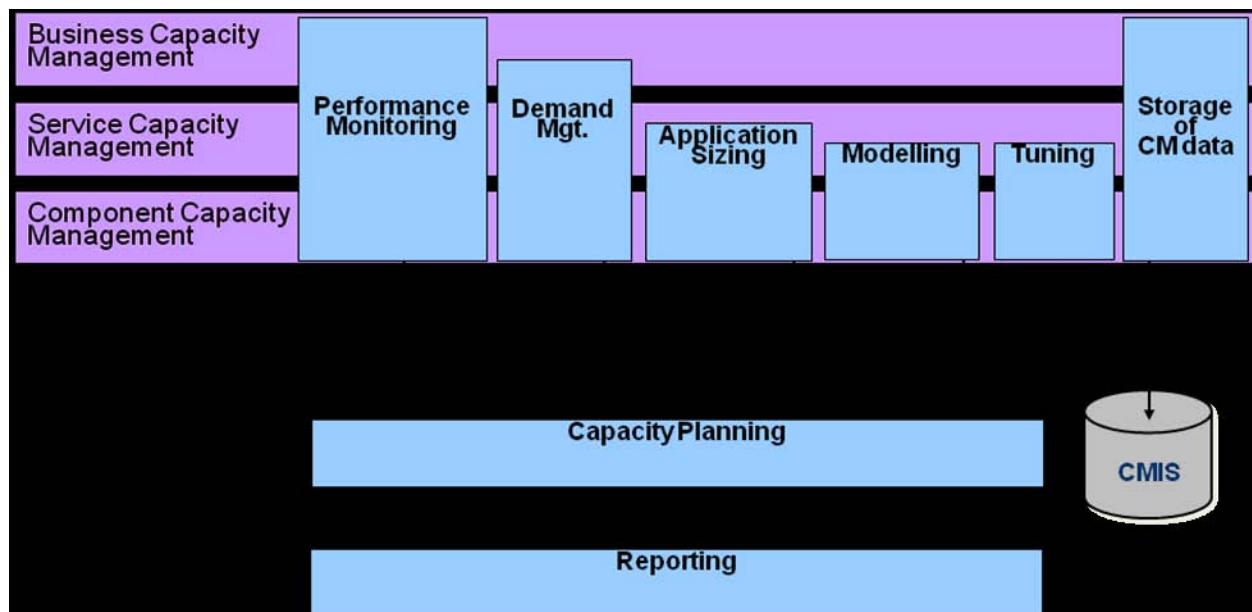


Figure 5.K – Activities of Capacity Management

Capacity Management consists of these main activities:

1. **Performance Monitoring** - Measuring, monitoring, and tuning the performance of IT Infrastructure components.
2. **Demand Management** - Short term reactive implementation of strategies considered in Service Strategy to manage current demand
3. **Application Sizing** - Determining the hardware or network capacity to support new or modified applications and the predicted workload.
4. **Modelling** - Used to forecast the behaviour of the infrastructure under *certain conditions*. (e.g. *if the number of users doubled, if a network link fails*)
5. **Tuning** – Modifications made for better utilizations of current infrastructure
6. **Storage of Capacity Management Data**
7. **Capacity Planning**
8. **Reporting**

Roles and Responsibilities for Capacity Management:

Capacity Manager

Responsibilities:

- Ensure adequate performance and capacity for all IT services
- Capacity Plan (development and management)
- Oversee Performance and Capacity monitoring & alerting
- Report provision and advice

Skills:

- Strategic business awareness
- Technical and analytical acuity
- 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 utilizes information from and provides information to all phases of the Service Lifecycle.

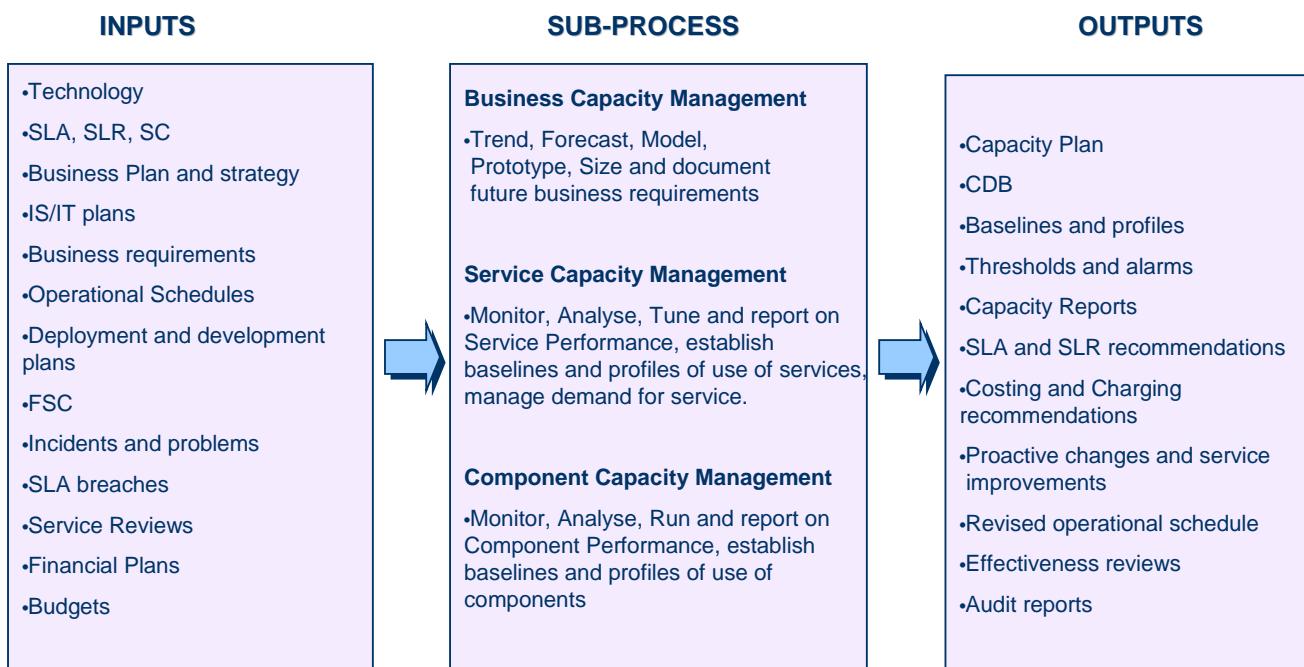


Figure 5.L – Capacity Management relationships with other areas of IT Service Management

5.3.5 Availability Management

GOAL: The primary goal of Availability Management is to ensure that the level of service availability delivered in all services is matched to or exceeds the current and future agreed needs of the business in a cost-effective manner.

Other Availability Management objectives are:

- Reduction in the frequency and duration of Availability related incidents;
- To maintain a forward looking Availability plan.

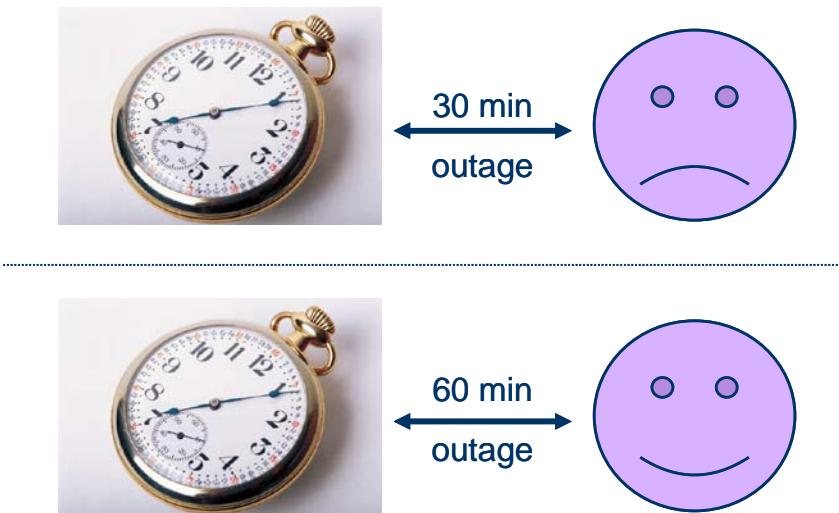


Figure 5.M – The user perception of Availability

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

A1: 30min outage during peak time, overtime being paid to staff, urgent report required.

A2: 60min outage on weekend, holiday, off peak, when service not required.

A3: 30min outage on critical IT Service, 60min outage on non-critical IT Service.

A4: 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.

Proactive and Reactive Elements of Availability Management:

Proactive activities: (Service Design Phase)	Reactive activities: (Service Operation Phase)
--	--

Terminology	Explanation
Availability:	The ability of an IT Service or component to perform its required function at a stated instant or over a stated period of time.
Security:	Services, systems and information should be made available to the authorized users at the authorized times. (See Information Security Management and Access Management)
Reliability:	Freedom from operational failure.
Resilience:	The ability to withstand failure . (e.g. through redundant components)
Maintainability: (internal)	The ability of an IT component to be retained in or restored to, an operational state. This will be affected by the skills, knowledge and availability of IT staff, as well various ITSM tools for detecting and managing disruptions.
Serviceability: (external)	The contractual arrangements made with external suppliers that document their obligations for supporting the availability of services. Measured by Availability, Reliability and Maintainability of IT Service and components under control of the external suppliers.
Vital Business Function (VBF):	The business critical elements of the business process supported by an IT Service. Typically this will be where more effort and investments will be spent to protect these vital business functions.

Activities:

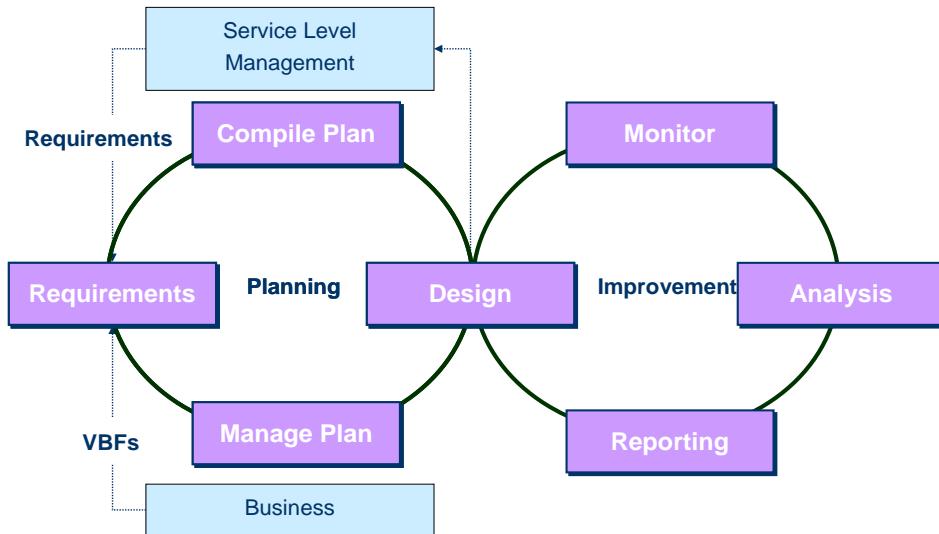


Figure 5.N – Availability Activities

Activities involved in Availability Management can form two continuous cycles of Planning and Improvement.

Availability Management and Incident Management:

An aim of Availability Management is to ensure the duration and impact from Incidents impacting IT Services are minimised, 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.

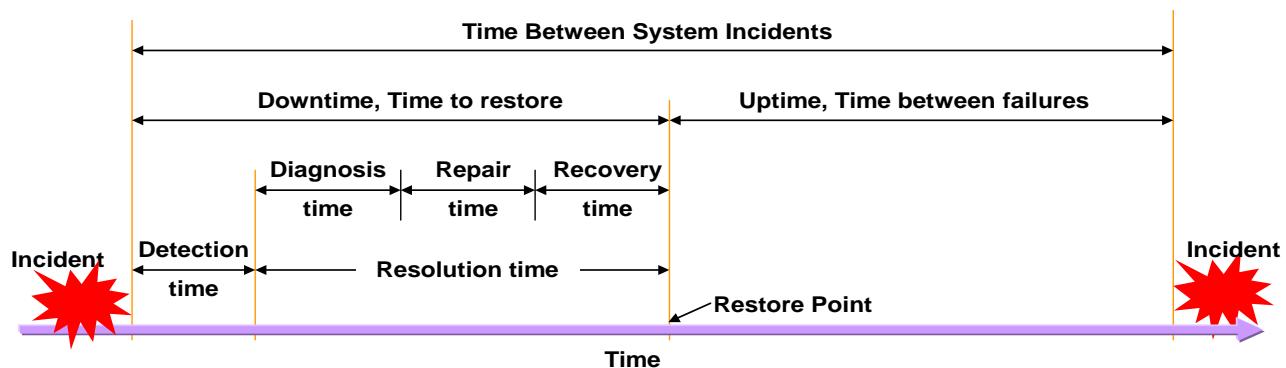


Figure 5.O – The Expanded Incident Lifecycle

Lifecycle of an Incident (Availability Management Metrics):**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 between the above terms

- High ratio of MTBF/MTBSI indicates there are many minor faults
- Low ratio of MTBF/MTBSI indicates there are few major faults

Other elements of the Expanded Incident Lifecycle:**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 the service provider restores 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 for Availability Management:

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 and analytical acuity
- Consultancy
- Seeks continuous improvement

NOTE: The Availability Manager does not seek to achieve 100% Availability, but instead seeks to deliver Availability that matches or exceeds (within reason) the agreed business requirements.

Key Performance Indicators of Availability Management:

Typical metrics for evaluation 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

5.3.6 IT Service Continuity Management

GOAL: To support the overall *Business Continuity Management* by ensuring that the required IT infrastructure and the IT service provision can be recovered within required and agreed business time scales.** Often referred to as Disaster Recovery planning. **

Terminology	Explanation
Disaster:	NOT part of daily operational activities and requires a separate system . (Not necessarily a flood, fire etc. but may be due to a blackout or power problem and the SLAs are in danger of being breached).
Business Continuity Management: (BCM)	Strategies and actions to take place to continue Business Processes in the case of a disaster. It is essential that the ITSCM strategy is integrated into and a subset of the BCM strategy.
Business Impact Analysis: (BIA)	Quantifies the impact loss of IT service would have on the business.
Risk Assessment:	Evaluate <i>Assets, threats and vulnerabilities</i> that exist to business processes, IT services, IT infrastructure and other assets.
Scope:	The scope of IT Service Continuity Management considers all identified critical business processes and IT service(s) that underpin them. This may include IT staff members, hardware, software, essential services and utilities, critical paper records, courier services, voice services & physical location areas e.g. offices, data centres etc.
	Typically the focus when implementing IT Service Continuity Management is to provide continuity strategies for identified vital business functions, however over time this scope should be expanded appropriately to a wider range of services.

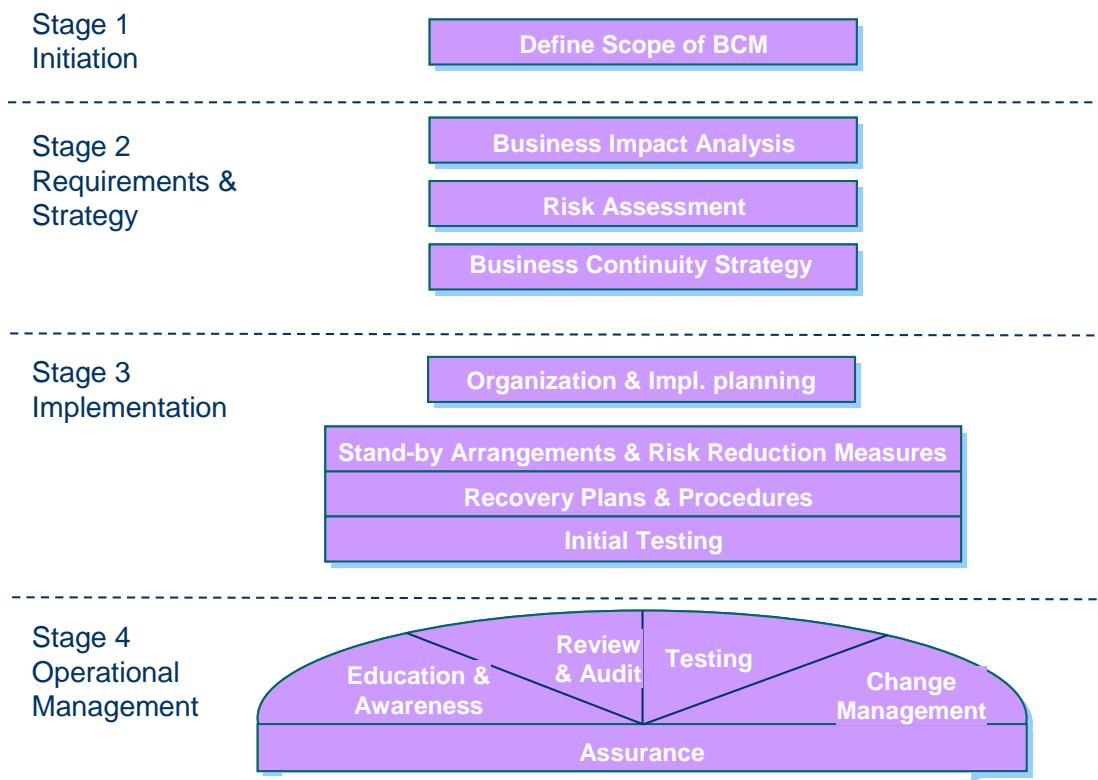


Figure 5.P – Activities of IT Service Continuity Management
 © Crown Copyright 2007 Reproduced under license from OGC

Key Activities of IT Service Continuity Management:

Performing a Business Impact Analysis (BIA) identifies:

- Critical business processes & 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 & external sources (the likelihood of occurring)
- Vulnerabilities (the extent of impact or effect on organization)

Developing Countermeasures (Recovery and Risk Reduction Measures):

Terminology	Explanation
Counter Measures:	Measures to prevent or <i>recover</i> from disaster
Manual Workaround:	Using <i>non-IT</i> based solution to overcome IT service disruption
Gradual recovery:	Aka <i>Cold</i> standby (>72hrs to recover from a 'Disaster')
Intermediate Recovery:	Aka <i>Warm</i> standby (24-72hrs to recover from a 'Disaster')
Immediate Recovery:	Aka <i>Hot</i> standby (< 24hrs, usually implies 1-2 hrs to recover from a 'Disaster')
Reciprocal Arrangement:	Agreement with another similar sized company to share disaster recovery obligations

Operational Management:

- Education & awareness
- 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:

Role	Responsibilities and Skills
Board	Crisis management Corporate / business decisions External affairs
Senior Management	Coordination 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

Typical responsibilities for ITSCM in planning and dealing with disaster are similar to how First Aid Officers and Fire Wardens act in planning and operational roles.

Skill requirements for ITSCM Manager and staff include:

- Knowledge of the business (help set priorities)
- Calm under pressure
- Analytical (problem solving)
- Leadership and Team players
- Negotiation and Communication

5.3.7 Information Security Management

GOAL: To align IT security with business security and ensure that information security is effectively managed in all service and IT Service Management activities.

Security objectives are met when:

- Information is available and usable when required, and the systems that provide it can appropriate resist attacks and recover from or prevent failures (availability)
- 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)
- Business transactions, as well as information exchanges between enterprises, or with partners, can be trusted (authenticity and non-repudiation)

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.

Terminology	Explanation
Confidentiality:	Protecting information against unauthorized access and use. Examples: <i>Passwords, swipe cards, firewalls</i>
Integrity:	Accuracy, completeness and timeliness of services, data information, systems and physical locations. Examples: <i>Rollback mechanisms, test procedures, audits.</i>
Availability:	The information should be accessible at any agreed time. This depends on the continuity provided by the information processing systems. Examples: <i>UPS, resilient systems, Service desk hours</i>

Terminology	Explanation
Security Baseline:	The security level adopted by the IT organization for its own security and from the point of view of good 'due diligence'. Possible to have multiple baselines Examples: <i>Security access based employee rank/title</i>
Security Incident:	Any incident that may interfere with achieving the SLA security requirements; materialization of a threat Examples: <i>Security Breach or potential weakness</i>



Figure 5.Q – Factors influencing Information Security Management

Information Security Management (ISM) needs to be considered within the overall corporate governance framework. This 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 the enterprise information resources are used responsibly.

The purpose of ISM is to provide a focus for all aspects of IT security and manage all IT activities.

Activities:

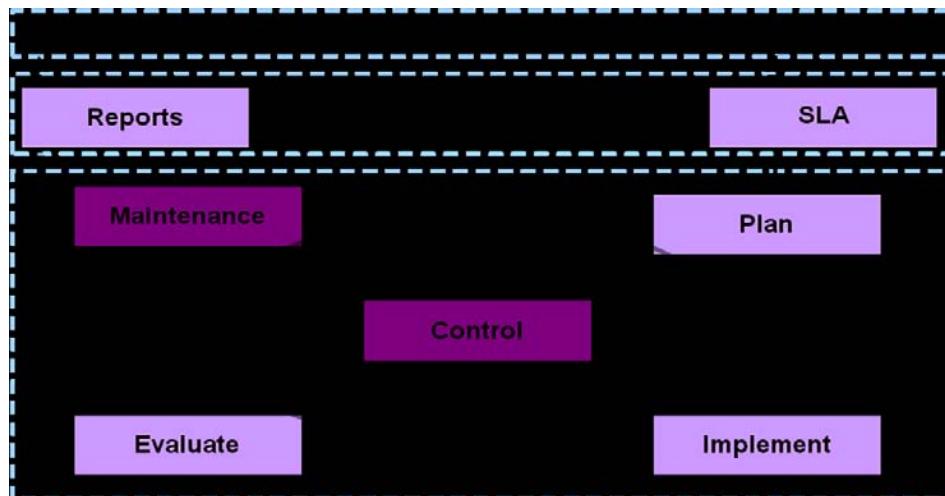
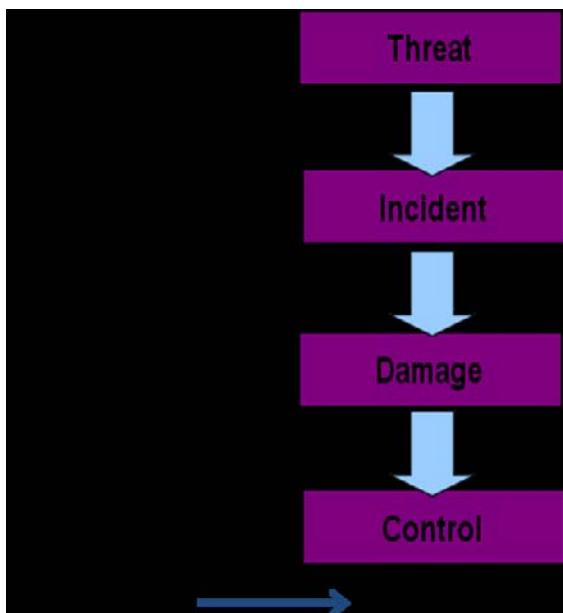


Figure 5.R – Activities of Information Security Management

Control:

The activity of Control has a central place in figure 5.M, as this is where Information Security is actually enforced in an organization. The way in which this is done is shown below.



- There are various security threats to our infrastructure and we want to prevent or reduce the damage of these as much as possible.
- In the case that they do pass our prevention mechanisms, we need to have detection techniques to identify when and where they occurred.
- Once a security incident has occurred, we want to repress or minimize the damage associated with this incident. We then want to correct any damage caused and recover our infrastructure to normal levels.
- After this process we need to review how and why the breach occurred and how successful were we in responding to the breach.

Figure 5.R – Control Mechanisms

Roles and Responsibilities for Information Security Management:

Responsibilities:

- Manage entire security process
- Consult with senior management

Skills:

- Strategic Sense of PR
- Tactical

Roles and Responsibilities for Security Officer:

Responsibilities:

- Day to day operational duties
- Advise staff on security policy and measures

Skills:

- Analytical
- Eye for detail
- Consultancy

Perspectives				
	Organizational	Procedural	Technical	Physical
Measures				
Prevention Reduction				
Detection				
Repression				
Correction				
Evaluation				

Figure 5.S – Activities of Information Security Management

The Information Security Measure Matrix is a useful tool in performing a gap analysis:

- Ensures there is a balance in measures
- Avoids a concentration of measures in either a certain perspective (e.g. technical) or of a certain measure (e.g. detection).

Remember: Ultimately it's a cost-benefit analysis that determines how much you invest in security.

5.4 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

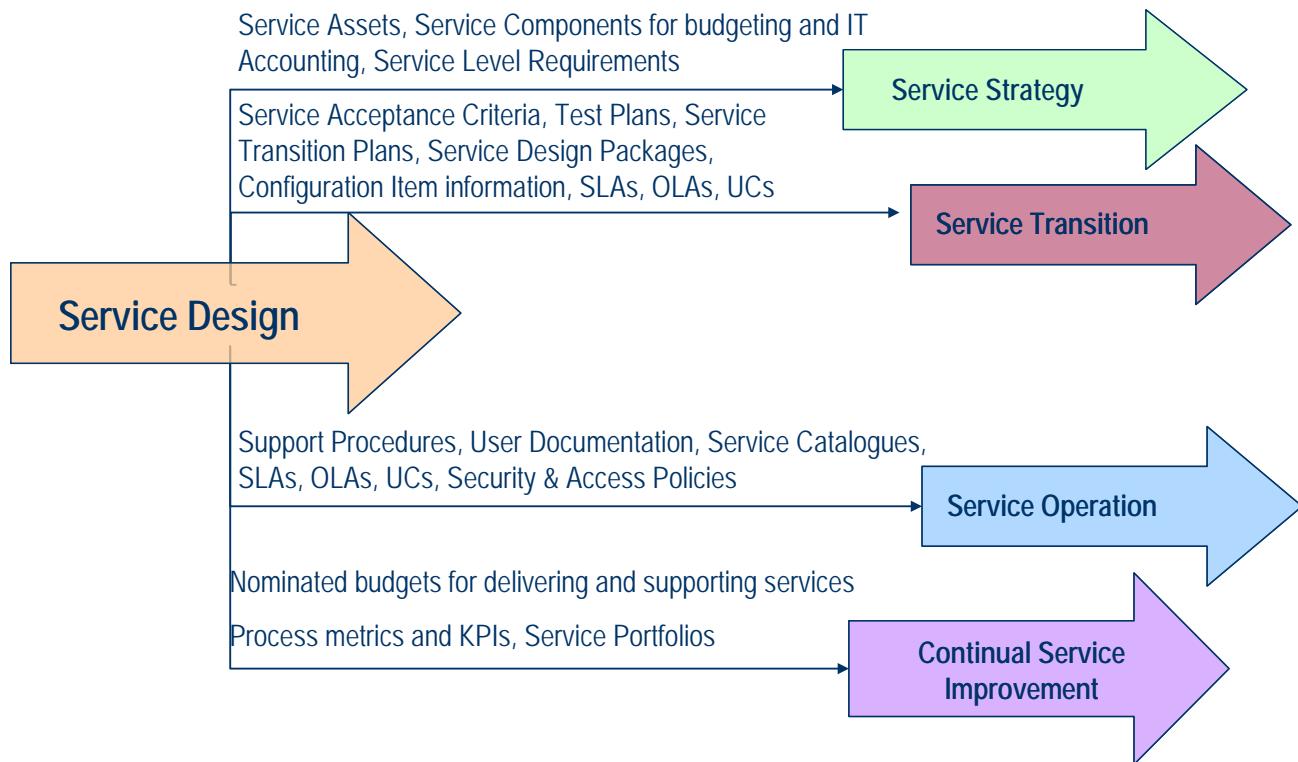


Figure 5.T – Some Service Design outputs to other lifecycle phases.

5.5 Service Design Scenario

5.5.1 Service Level Management Considerations

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

5.5.2 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

5.5.3 Availability Management Considerations

- To ensure availability targets are met, regular maintenance of components required, as well as ensuring through Supplier Management that ISP UC is met (serviceability requirements).
- If business wants 24/7 access, then design of redundant systems may be required... at a cost!

5.5.4 Information Security Management Considerations

- **Confidentiality** – user passwords design (e.g. HYPE service is not controlled locally – all information is stored on vendor's servers. If all users use same password as network login, resulting in a clear pattern, then it would be possible for security to be threatened if "someone" hacked into vendor 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

5.5.5 Service Catalogue Management Considerations

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

5.5.6 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

5.5.7 Supplier Management Considerations

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

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

5.6 Service Design Review Questions

5.6.1 Question 1

Which ITIL® process analyses 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 & Configuration Management

5.6.2 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

5.6.3 Question 3

In which ITIL® process are negotiations held with the customer 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

5.6.4 Question 4

Which of the following BEST describes a Virtual Service Desk structure?

- a) A Service Desk that also provides onsite technical support to its users
- b) A Service Desk where analysts only speak one language
- c) A Service Desk that is situated in the same location as the users it serves
- d) A Service Desk that could be in any physical location but uses telecommunications and systems to make it appear that they are in the same location

5.6.5 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

5.6.6 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

5.6.7 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

5.6.8 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 fallback arrangements
- c) reporting regarding availability
- d) guaranteeing that the Configuration Items are constantly kept up-to-date.

5.6.9 Question 9

Information security must consider the following four perspectives:

I. Organizational

II. Physical

III. Technical, and

IV. ...

- a) Process
- b) Security
- c) Procedural
- d) Firewalls

5.6.10 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 base, multi-level based

6 Service Transition

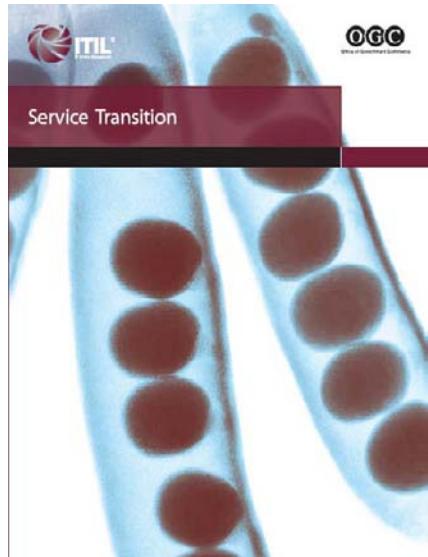


Figure 6.A: Service Transition

The Service Transition lifecycle phase focuses on the vulnerable transition between the Design phase and the Operation phase of a service. It is particularly critical as functional and technical errors not found during this phase 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:

- Knowledge Management
- Service Asset & Configuration Management
- Change Management
- Release & Deployment Management
- Service Validation and Testing

6.1 Objectives

The primary objective of Service Transition is the development and improvement of capabilities for transitioning new and modified services into operation.

Other objectives include:

- To ensure that new and changed services meet customer requirements and do not adversely impact the IT infrastructure or business processes.
- To reduce the variation between estimated and actual costs, timeframes, risks and impact scales.
- To build, configure, test and deploy quality Releases into operation in the most efficient manner while also minimising disruption to the business and customers.

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 and other resources against those estimated in budgets.

6.2 Service Transition Processes

6.2.1 Knowledge Management

GOAL: To enable organizations to improve the quality of management decision making by ensuring that reliable and secure information and data is available throughout the service lifecycle.

The primary purpose is to improve efficiency by reducing the need to rediscover knowledge. This requires accessible, quality and relevant data and information to be available to staff.

Benefits that a successful Knowledge Management System would deliver to the business and IT organization:

- We can stop having to continually reinvent the wheel
- More efficient use of resources (including people)
- Enables the organization to continually mature and develop

Challenges you would see in implementing and operating a Knowledge Management System:

- Getting staff to use the systems;
- Having the extra time required to record relevant information and knowledge after actions are made;
- Managing information and knowledge that is no longer correct or relevant for the organization;
- Designing a system that can scale well as an organization grows.

One of the more difficult components of Knowledge Management is ensuring that we do more than simply capture discrete facts about various elements of the organization and IT infrastructure. What this requires is an understanding of the different components and processes required to develop and mature knowledge and wisdom.

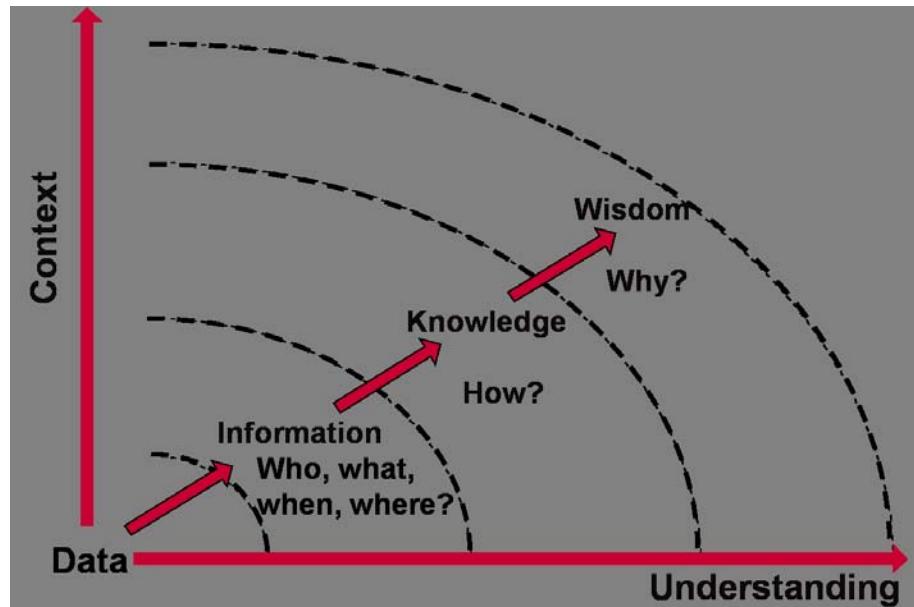


Figure 6.B – Moving from data to wisdom
 © Crown Copyright 2007 Reproduced under license from OGC

Data:

Data is a set of discrete facts. Most organizations capture significant amounts of data every day.

Information:

Information comes from providing context to data. This usually requires capturing various sources of data and applying some meaning or relevance to the set of facts.

Knowledge:

Knowledge is composed of the experiences, ideas, insights and judgments from individuals. This usually requires the analysis of information, and is applied in such a way to facilitate decision making.

Wisdom:

Gives the ultimate discernment of the material and having the application and contextual awareness to provide a strong common sense judgment. The use of wisdom ultimately enables an organization to direct its strategy and growth in competitive market spaces.

We can use tools and databases to capture Data, Information and Knowledge, but Wisdom cannot be captured this way, as Wisdom is a concept relating to abilities to use knowledge to make correct judgments and decisions.

Components, Tools and Databases

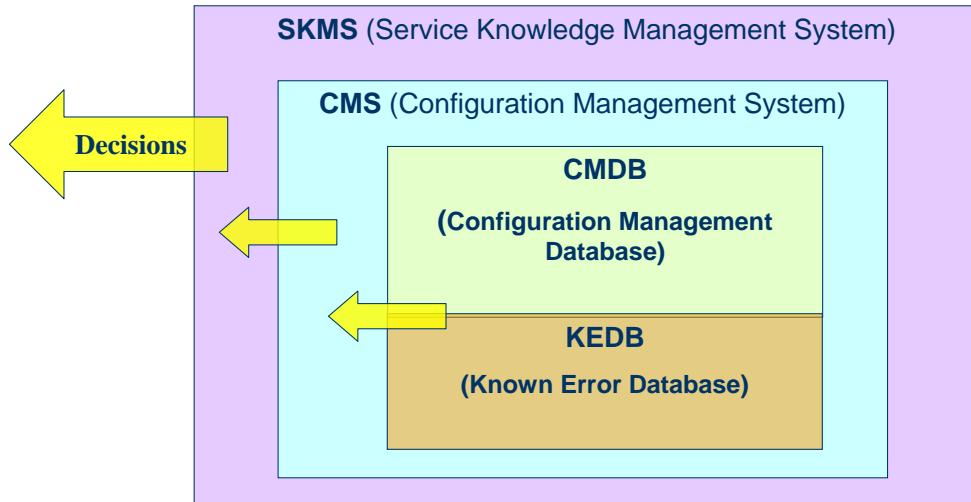


Figure 6.C – Components making up the Service Knowledge Management System
 (Note the relevant size of each box, which indicates the relative scope of data, information and knowledge captured)

SKMS: Service Knowledge Management System (SKMS):

The complete set of integrated repositories that are used to manage knowledge and information. The SKMS includes 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.

CMS: Configuration Management System:

A set of tools and databases that are used to manage an IT service provider's configuration data. The CMS also includes information about incidents, problems, known errors, changes and releases; and may contain data about employees, suppliers' locations, business units, customers and users. The CMS is maintained by Service Asset & Configuration Management and is used by all IT Service Management processes. Two major components are the:

- **CMDB:** Configuration Management Database. Stores configuration details for the IT infrastructure
- **KEDB:** Known Error Database. This database is created by Problem Management and used by Incident and Problem Management.

6.2.2 Service Asset and Configuration Management

GOAL: To support the agreed IT service provision by *managing, storing and providing information* about Configuration Items (CI's) and Service Assets throughout their life cycle. This assists in providing a logical model of the infrastructure, including the relevant relationships and dependencies that exist.

This process manages the details of service assets and Configuration Items in order to support the effectiveness and efficiency of other Service Management processes.

Terminology	Explanations
Configuration Item (CI):	<p>Reference to ANY component that supports an IT service (except people).</p> <p><i>Example: IT components or associated items such as Request for Changes, Incident Records, Service Level Agreements.</i></p>
Attribute:	<p>Specific information about CI's that are appropriate to maintain.</p> <p><i>Example: Size of RAM, hard drive, bandwidth</i></p>
CI Level:	Recording and reporting of CI's at the level that the business requires without being overly complex. It's a trade-off balancing the value that the information will provide versus the effort and cost to manage the information over time (<i>not too much or too little</i>).
Status Accounting:	Reporting of all current and historical data about each CI throughout its lifecycle. <i>Example: Status = Under Development, being tested, live, withdrawn etc</i>
Configuration Baseline:	Configuration details captured at a specific point in time. This captures both the structure and details of a configuration, and is used as a reference point for later comparison (e.g. After major changes, disaster recovery etc)

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.

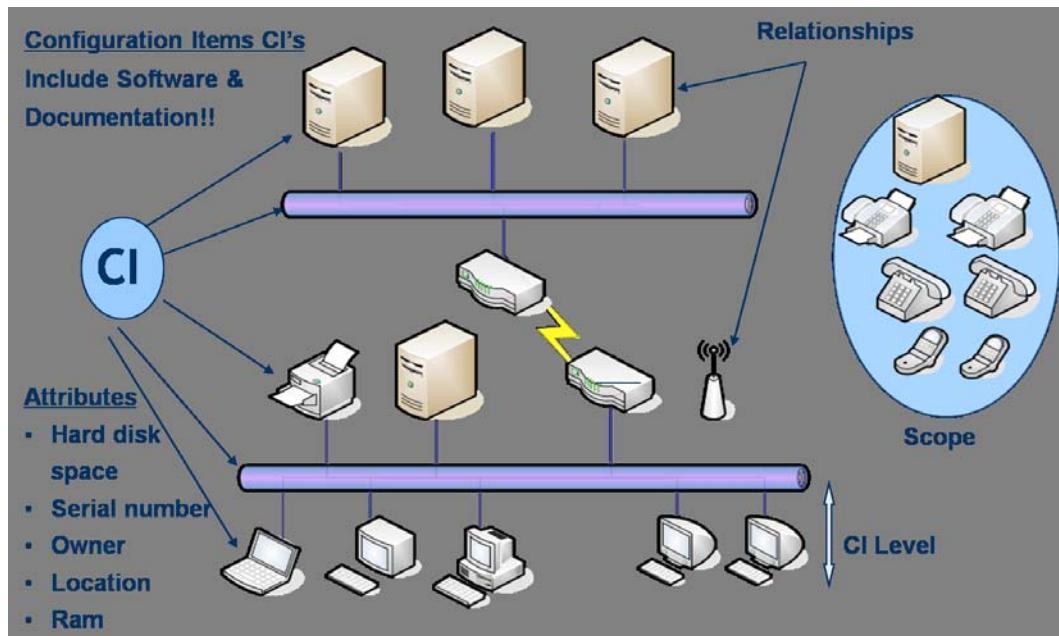


Figure 6.D – The Configuration Management Database (CMDB)

As shown, it is important to determine what 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 – Configuration Management Activities

Notice how MANAGEMENT & PLANNING are the central activities. Good, sound Service Asset & 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 & 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: The selection, identification, labelling 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 – include 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
- Update of CI records and licence control
- Updates in connection with RFCs and Change Management
- Update 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

The benefits of the CMDB (not necessarily one physical database):

- One tool and not several tools → reduced costs
- Consistent and visible information about the IT infrastructure available to all staff
- One team and not several support teams → reduced costs, improved consistency in CI management
- One stop shop for Configuration queries
- The data about CIs and methods of controlling CIs is consolidated -> reduces auditing effort
- Opens opportunities for consolidation in CIs to support services

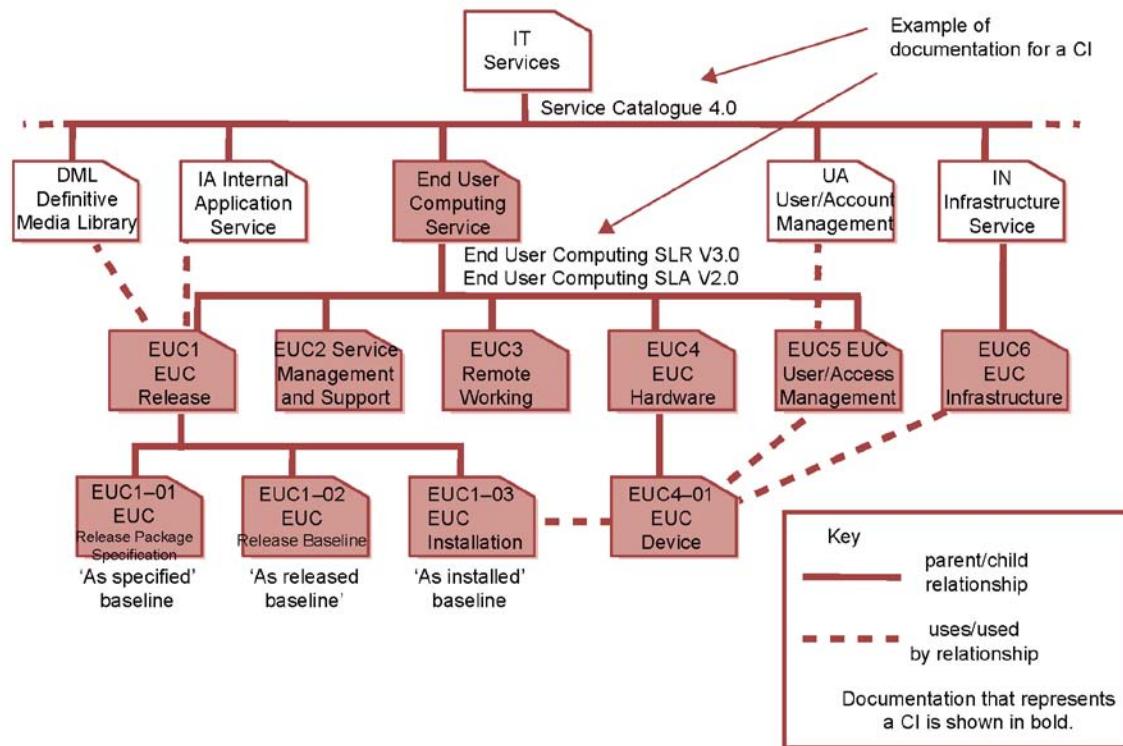


Figure 6.F – Example configuration breakdown for an IT Service
 © Crown Copyright 2007 Reproduced under license from OGC

Roles and Responsibilities:

Service Asset Management

The management of service assets across the whole lifecycle including:

- Full lifecycle management of IT and service assets from acquisitions to disposal
- Maintenance of the asset inventory.

Configuration Management:

- To provide a logical model of the services, assets and infrastructure by recording the relationships between service assets and configuration items
- To ensure control procedures are complied with to protect the integrity of Configurations.
- To support the information needs of other ITIL® processes

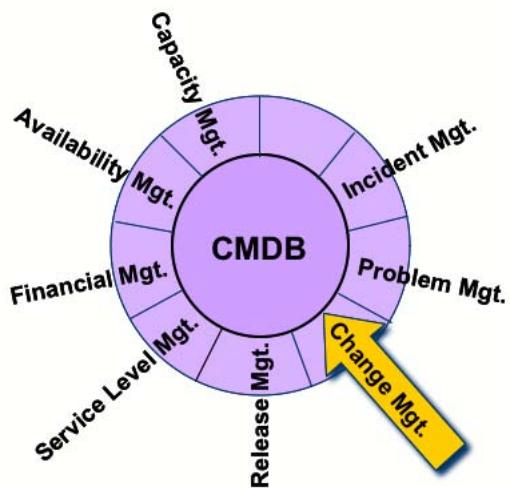
The actual roles related to Service Asset and Configuration Management include:

- Service Asset Manager
- Configuration Manager
- Configuration Analyst
- Configuration Administrator/Librarian
- CMS/Tools Administrator
- Change Manager (all Changes to CIs must be authorized by Change Management)

6.2.3 Change Management

GOAL: To ensure that **standardized methods and procedures** are used for controlled, efficient and prompt handling of all Changes, in order to **minimize the impact** of Change-related Incidents upon service quality, and consequently to improve the day-to-day operations of the organization.

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



Change Management acts as the greatest contributor to the CMDB, as Changes to 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.

Terminology

Explanations

Change:

ANY alteration in the state of a defined Configuration Item. This includes the addition, modification or removal of approved, supported or baselined hardware, network, software, application, environment, system, desktop build or associated documentation.

Change Models:

Defines how various categories of changes are assessed & authorized, with different mechanisms and activities used to process and deliver changes based on the change type.

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.

Terminology	Explanations
STANDARD Change:	A <i>pre-approved</i> 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 .
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.
Request for Change: (RFC)	Standard form to capture and process ALL Changes to any CI
Change Schedule:	Schedule of Approved Changes and their proposed implementation dates. The Service Desk should communicate this to the users.
Projected Service Outage (PSO):	Details of revised targets for agreed SLAs and service availability because of changes being implemented in addition to planned downtime from other causes such as planned maintenance and data backups.
Change Advisory Board: (CAB)	A group that provides expert advice to the Change Manager. Involves representatives from various IT and business areas as well as other involved stakeholders including external suppliers. Chaired by the Change Manager
Emergency CAB: (ECAB)	Subgroup of CAB to provide expert advice for emergency change decisions.

Activities:

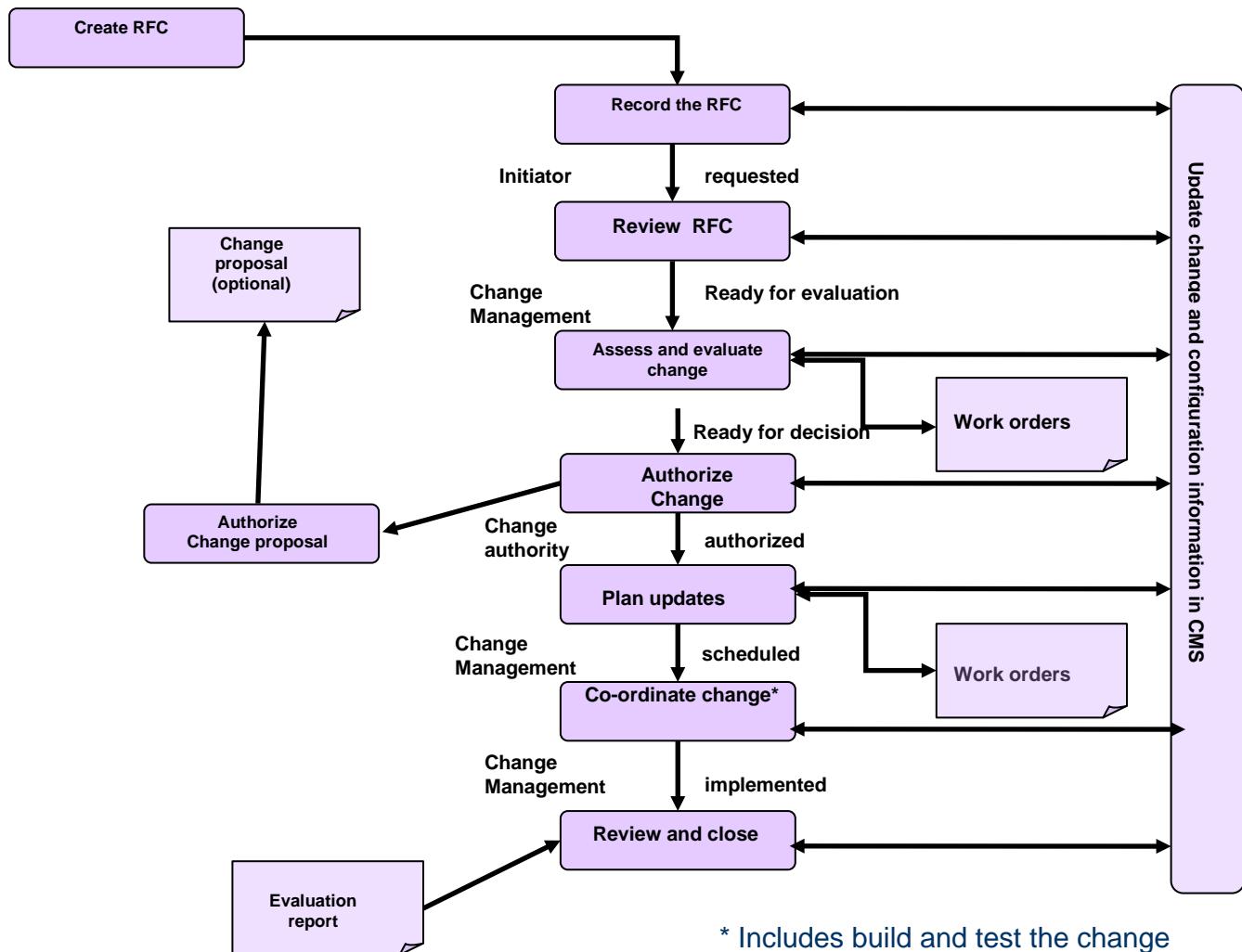


Figure 6.G– The Activities of Change Management
 © Crown Copyright 2007 Reproduced under license from OGC

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. This is authorized by the Change Manager
5. Work orders are issued for the build of the Change (carried out by other groups)
6. Change Management coordinates the work performed (with multiple checkpoints)
7. The Change is reviewed
8. The Change is closed

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.

Impact: **Typical Escalation Level:**

- Standard Executed using a pre-defined form/template

Normal Changes

- Minor Change Manager (CM) or other operational process manager
- Significant Change Advisory Board (CAB)
- Major IT Management Board

Urgency:

- Normal Change Manager or CAB
- Emergency Emergency CAB Committee (ECAB)

The 7Rs of Change Management:

When assessing Changes, it is important to have answers to the following seven questions:

- Who RAISED the change?
- What is the REASON for the change?
- What is the RETURN required from the change?
- What are the RISKS involved in the change?
- What RESOURCES are required to deliver the change?
- Who is RESPONSIBLE for the build, test and implementation of the change?
- What is the RELATIONSHIP between this change and other changes?

These questions must be answered for ***all changes***. Without this information the impact assessment cannot be completed, and the balance of risk and benefit to the live service will not be understood. This could result in the change not delivering all the possible or expected business benefits or even of it having a detrimental, unexpected effect on the live service.

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's it going to cost? And what's the cost of not doing it?
- Business Approval - What are the consequences to the business? And not doing it?
- Technology Approval - What are the consequences to the infrastructure? And 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:

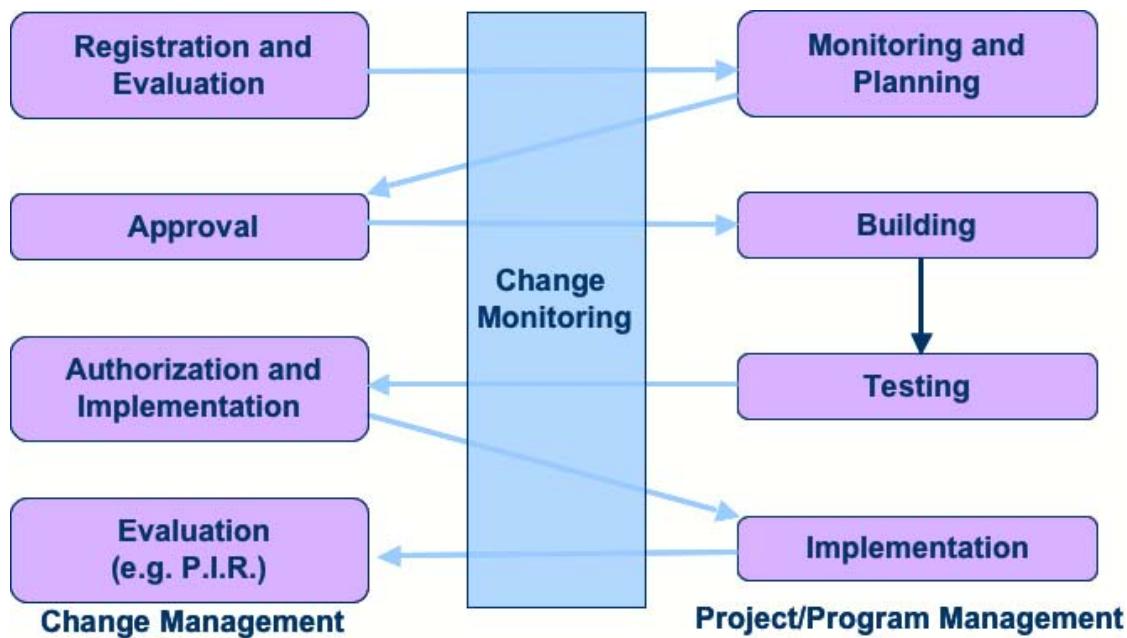


Figure 6.H Relationship with Project Management

© Crown Copyright 2007 Reproduced under license from OGC

How does Change Management work with Project Management?

- Change Management authorizes, controls, coordinates, but **does not** plan, build, test or implement changes itself
- 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, FSC for Service Desk
- Authorize (or reject) changes

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.

Release and Deployment Manager

- Manages the release of changes
- Advises the Change Manager (as part of CAB) on release issues

Technical Specialists

- Build, test and deploy the actual hardware and software change components.

Key Performance Indicators (KPIs) of Change Management

It is important that a balanced view of metrics is used when assessing the effectiveness and efficiency of the Change Management process. These metrics include:

- Number of RFCs (Accepted/Rejected)
- Number and % of successful Changes
- Emergency Changes
- Number of Changes awaiting implementation
- Number of implemented Changes
- Change backlogs and bottle-necks
- Business impact of changes
- Frequency of Change to CIs

Challenges affecting Change Management

- Change in culture – Now one central process comes into place that influences everyone's activities
- Bypassing - projects ducking the Change Management planning
- Optimal link with Configuration Management - to execute a controlled change all data MUST be reliable
- Commitment of the supplier(s) to the process
- Commitment of senior management.

6.2.4 Release and Deployment Management

GOAL: To deploy new releases into production, transition support to service operation, and enable its effective use in order to deliver value to the customer.

Terminology	Explanations
Release:	A collection of authorized Changes to an IT Service.
Release Unit:	A Release Unit describes the portion of a service of IT infrastructure that is normally released together according to the organization's release policy. The unit may vary depending on type(s) or item(s) of service asset or service component such as hardware or software.
Release Package:	A release package may be a single release unit or a structured set of release units, including the associated user or support documentation that is required.
Definitive Media Library (DML): <i>(previously known as the DSL)</i>	The secure library in which the definitive authorized versions of all media CIs are stored and protected. The DML should include definitive copies of purchased software (along with license documents or information) as well as software developed on site.
Definitive Spares (DS): <i>(previously known as DHS)</i>	Physical storage of all spare IT components and assemblies maintained at the same level as within the live environment . New IT assemblies are stored here until ready for use, and additional components can be used when needed for additional systems or in the recovery from Incidents. <ul style="list-style-type: none">• Details recorded in the CMDB, but controlled by Release and Deployment Management.
Early Life Support	Where release and deployment teams assist in managing any calls, incidents and problems that are detected in the immediate few days/weeks after the deployment of the new or modified service.

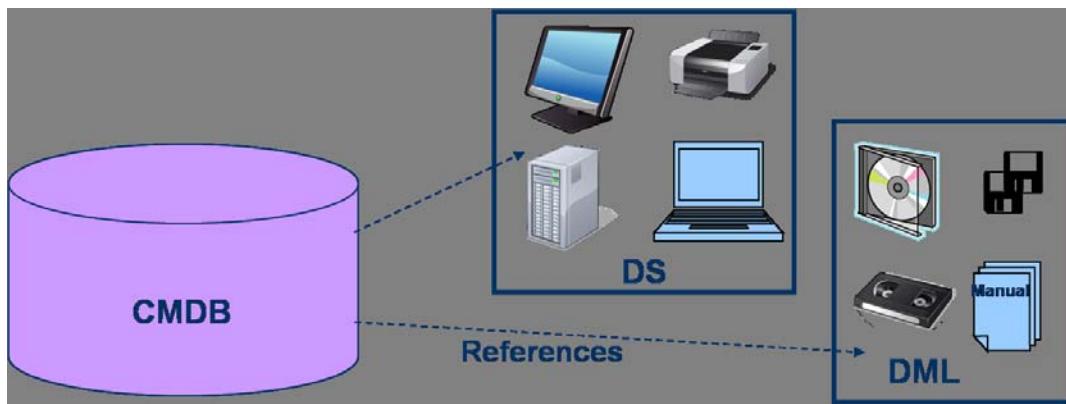


Figure 6.I – The Definitive Media Library and Definitive Spares

Remember – the elements found within the DML and DS are referenced by the CMDB as CIs.

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:

- email notification
- SMS notification
- verbal communication

Options for the deployment of Releases

Big Bang:

The new or changed service is deployed to all user areas in one operation. This will often be used when introducing an application change and consistency of service across the organization is considered important.

The negative aspect of the Big Bang approach is that it increases the risk and impact of a failed Release.

Phased Approach:

The service is deployed to a part of the user base initially, and then this operation is repeated for subsequent parts of the user base via a scheduled rollout plan.

This will be the case in many scenarios such as in retail organizations for new services being introduced into the stores' environment in manageable phases.

The Push Approach:

Is used where the service component is deployed from the centre and pushed out to the target locations.

In terms of service deployment, delivering updated service components to all users, either in big bang or phased form is using the push approach, since the new or changed service is delivered into the users' environment at a time not of their choosing.

The Pull Approach:

Used for software releases where the software is made available in a central location but users are free to pull the software down to their own location at a time of their choosing or when a workstation restarts.

Automated:

The use of technology to automate Releases. This helps to ensure repeatability and consistency. The time required to provide a well-designed and efficient automated mechanism may not always be available or viable.

Manual:

Using manual activities to distribute a Release. It is important to monitor and measure the impact of many repeated manual activities as they are likely to be inefficient and error prone.

Activities

Figure 6.J – Activities of Release & Deployment

Release Planning:

- Defining the Release contents
- Defining the Release Schedule
- Defining the resources, roles & responsibilities required for the Release

Design & Test (Coordinates with other Service Design and Service Transition Processes):

- Produce Release assembly & build instructions
- Create Installation scripts
- Run Test plans
- Develop Back-out procedures
- Produce tested installation procedures

Rollout Planning:

- Defining timetable for distribution
- Identification of affected CIs
- Defining communication plans
- Defining training plans
- Communication & training for:
 - Users
 - Support staff (including the Service Desk)

Logistics, Distribution & Installation:

During the actual implementation itself, the activities performed can be grouped under the following tasks:

1. Transfer financial assets
2. Transfer changes required to business/organization
3. Deploy processes and materials
4. Deploy Service Management Capability
5. Transfer service
6. Deploy service
7. Decommissioning and service retirement
8. Remove redundant assets

These activities will need to be modified to accommodate any items specified in the deployment plan as part of the acceptance criteria for 'go live'.

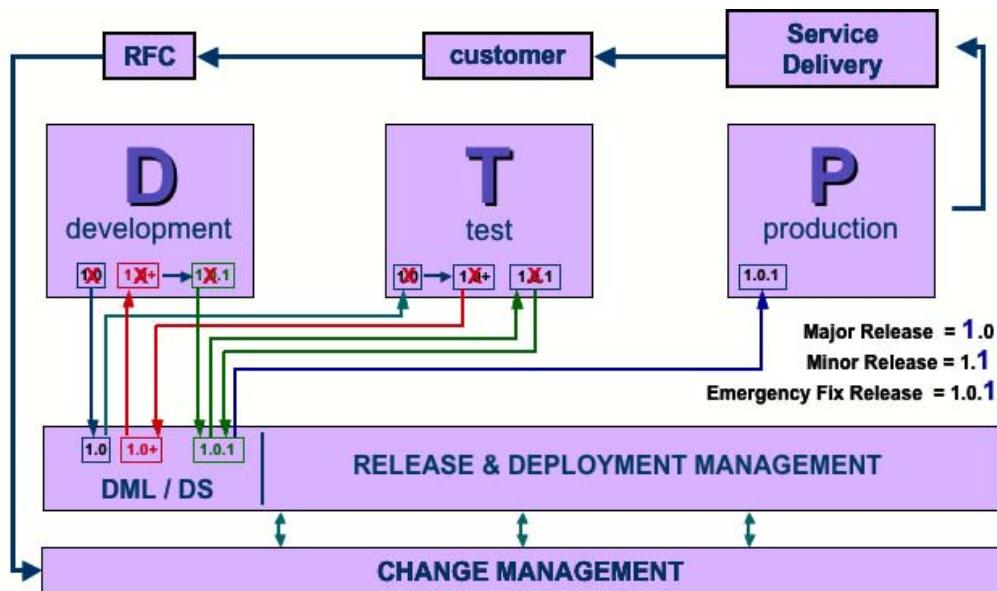


Figure 6.K - Transitioning New and Changed Services into Operation

Note how Change Management, Release & Deployment Management, Service Validation & Testing and Service Asset & Configuration Management work together for the transition of new or modified Services.

Roles and Responsibilities

Release & Deployment Manager:

- Drive effectiveness & efficiency of process
- Manage release management team
- Liaise with Change & Configuration Management, IT platform managers, Application Developers etc.

Skills

- Technical & coordination skills
- Project management

Release & Deployment Management Team

- Manage the DML & DS
- Design, build, test & deploy releases
- Manage software management/distribution tools

6.2.5 Service Validation and Testing

GOAL: The overriding goal of Service Validation and Testing is to assure that the new or modified service will provide the appropriate value to customers and their business. Other objectives include:

- Provide confidence that service changes deliver the expected outcomes and value for customers within the projected costs, capacity and constraints. This includes verification that the service is ‘fit for purpose’ and ‘fit for use’.
- Confirm that customer and stakeholder requirements and criteria are correctly defined and address and variances as early as possible.

The underlying concept to which Service Validation contributes is quality assurance – establishing that the service design and release will deliver a new or changed service or service offering that satisfies the requirements and standards of the customers and stakeholders involved.

Testing is a vital area within Service Management and has often been the unseen underlying cause of what was taken to be inefficient Service Management processes. If services are not tested sufficiently, then their introduction into the operational environment will bring rise in:

Incidents

- Failures in service elements and mismatches between what was wanted and what was delivered impact on business support;

Service Desk calls for assistance

- Services that are not functioning as intended are inherently less intuitive causing higher support requirements;

Problems and errors

- That are harder to diagnose in the live environment;

Costs

- Since errors are more expensive to fix in production than if found in testing;

Services that are not used effectively

- By the users to deliver the desired value.

The Service Validation and Testing process closely collaborates with other Service Transition processes as well as others from across the Service Lifecycle.

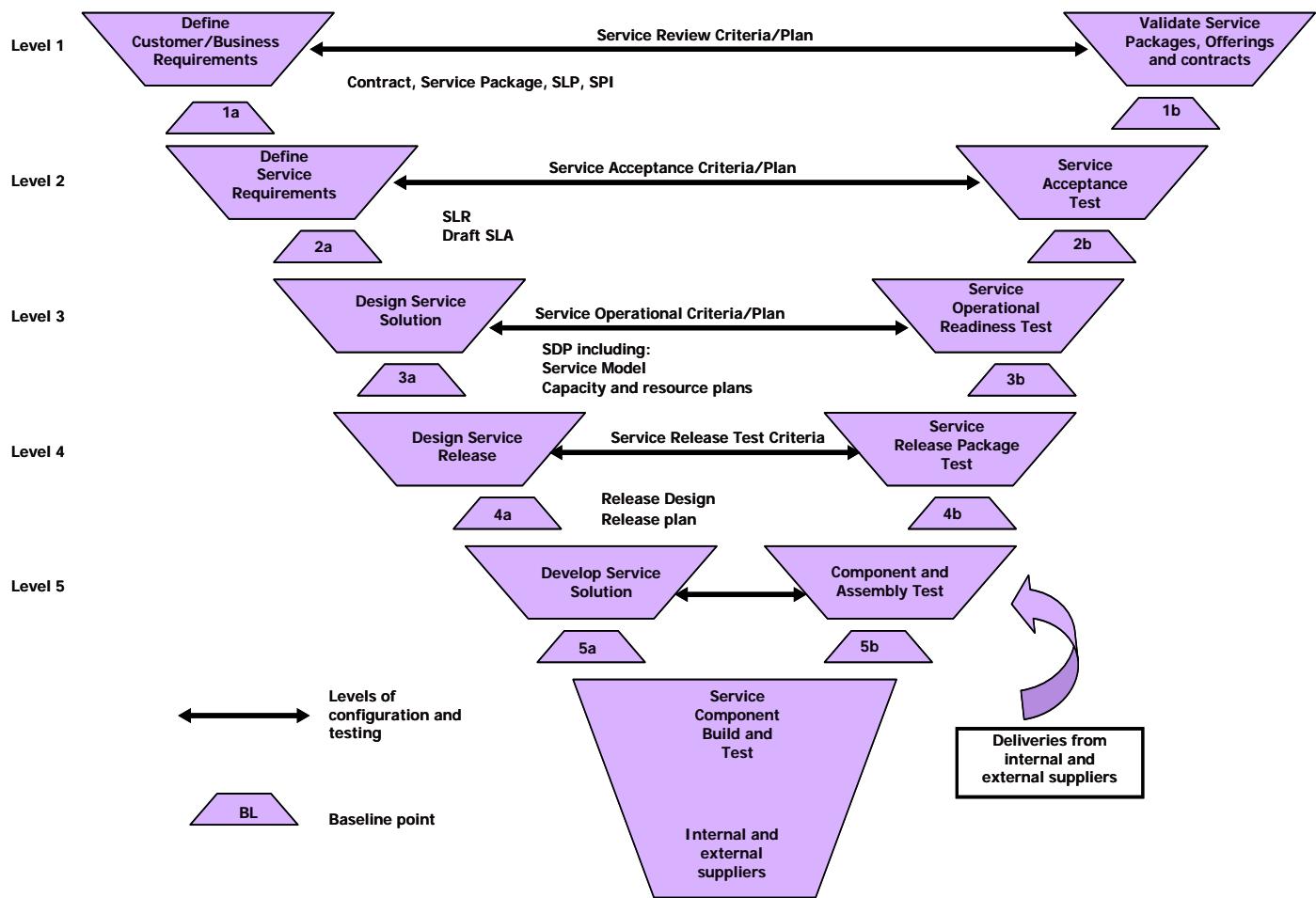


Figure 6.J – The Service V Model
© Crown Copyright 2007 Reproduced under license from OGC

The Service V Model is a concept of defining the appropriate requirements and appropriate validation methods that apply in order to **justify release to the customer for trial and assessment**.

- The **left hand side** represents the specification of the high-level business requirements, which gets further refined down to the detailed Service Design criteria and individual release package criteria.
- The **right hand side** focuses on the validation and test activities that are performed against the specifications defined on the left hand side, with direct involvement by the equivalent party on the right hand side (i.e. the person who signs off on the business requirements also signs to accept the service page has met their requirements)

Ideally, the design of a service will be performed in a top-down approach, yet testing will typically occur starting from the bottom and moving up.

6.3 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.

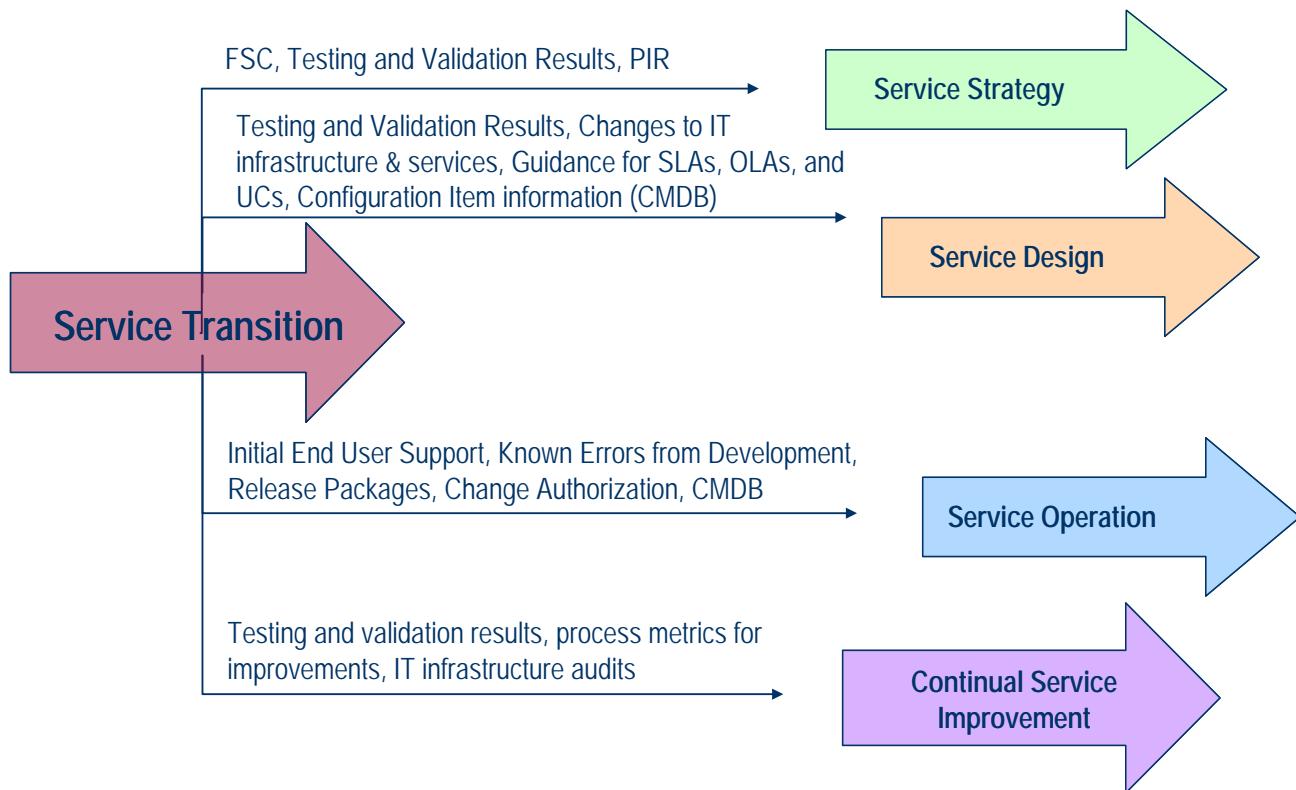


Figure 6.L – Some Service Transition outputs to other lifecycle phases.

6.4 Service Transition Scenario

6.4.1 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.

6.4.2 Service Asset and Configuration Management Considerations

- HYPE software is registered as 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

6.4.3 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 best path of action (through CAB).

6.4.4 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 – (in-services Service Desk 1st)

6.4.5 Service Validation and Testing Considerations

- Tests HYPE based on customer criteria – (set out in Service Design)
- looks at access, impact on live environment
- As stated previously, found RAM issues and referred back to Change via RFC
- Quality of components

6.5 Service Transition Review Questions

6.5.1 Question 1

Which process would you find the Service V model?

- a) Release Management
- b) Service Transition
- c) Service Validation and Testing
- d) Knowledge Management

6.5.2 Question 2

Release and deployment options include:

- 1. *Big bang vs. Phased*
 - 2. *Automated vs. Manual*
 - 3. ...
- a) Push vs. Proposed
 - b) Push vs. Pull
 - c) Requested vs. Forced
 - d) Proposed vs. Forced

6.5.3 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

6.5.4 Question 4

Which activity in Service Asset & Configuration Management would help to ascertain which Configuration Items conform to that which exists in the physical environment?

- a) control
- b) verification and audit
- c) identification
- d) status accounting

6.5.5 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 Programme (SIP)
- d) Service Level Requirement (SLR)

6.5.6 Question 6

Which of the following is not change type?

- a) Standard change
- b) Normal change
- c) Quick change
- d) Emergency change

6.5.7 Question 7

Which process is responsible for maintaining the DML?

- a) Release and Deployment Management
- b) Service Asset and Configuration Management
- c) Service validation and testing
- d) Change Management

6.5.8 Question 8

Which process or function is responsible for communicating the forward schedule of changes to the users?

- a) Change Management
- b) Service Desk
- c) Release and Deployment Management
- d) Service Level Management

6.5.9 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
- c) The end point of any project
- d) A rollback procedure

6.5.10 Question 10

The main objective of Change Management is to?

- a) Ensure that any changes are approved and recorded
- b) Ensure that standardised methods and procedures are used for controlled handling of all changes
- c) Ensure that any change requests are managed through the CAB
- d) Ensure that the CAB takes responsibility for all change implementation

7 Service Operation

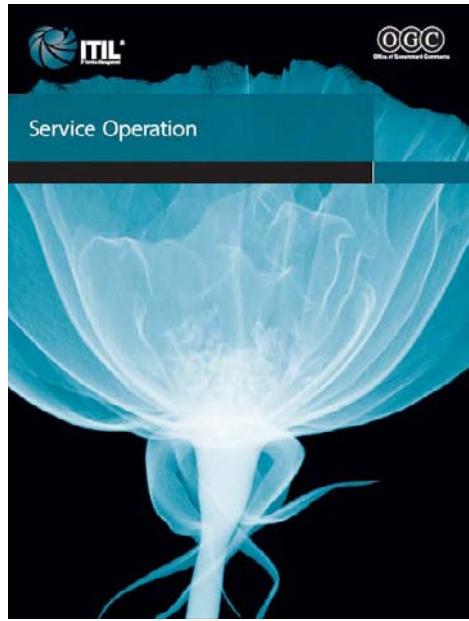


Figure 7.A – Service Operation

The Service Operation lifecycle phase is primarily focused on the management of IT Services that ensures effectiveness and efficiency in delivery and support.

Successful Service Operation requires coordination and execution of the activities and processes required to deliver and manage services at agreed levels to business users and customers. Service Operation is also responsible for ongoing management of the technology that is used to deliver and support services.

One of Service Operations 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.

7.1 Objectives

The primary objective of Service Operation is to enable effectiveness and efficiency in delivery and support of IT services. Strategic objectives are ultimately realized through Service Operations, therefore making it a critical capability. This lifecycle phase provides guidance on:

- How to provide stability in Service Operations, allowing for changes in design, scale, scope and service levels.
- Service Operation process guidelines, methods and tools for use in two major control perspectives; reactive and proactive. Managers and practitioners are provided with knowledge allowing them to make better decisions in areas such as managing the availability of services, controlling demand, optimizing capacity utilization, scheduling of operations and fixing problems.
- Supporting operations through new models and architectures such as shared services, utility computing, web services and mobile commerce.

7.2 Major Concepts

Achieving the Balance

Service Operation is more than just a repetitive execution of a standard set of procedures or activities, this phase 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.



Figure 7.B – Achieving a balance in Service Operation

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.	VS	External Business View: Focuses on the way in which services are experienced by its users and customers. An organization has business focus, but tends to under-deliver on promises to the business.
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	Responsiveness: Service Operation must recognize that the business and IT requirements change. When there is an extreme focus on responsiveness IT may tend to overspend on change and also decrease the stability of the infrastructure.

<p>Cost of Service:</p> <p>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.</p>	VS	<p>Quality of Service:</p> <p>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.</p> <p>The goal should be to consistently deliver the agreed level of IT service to its customer and users, while at the same time keeping costs and resource utilization at an optimal level.</p>
<p>Reactive:</p> <p>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 to ensure 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.</p>	VS	<p>Proactive:</p> <p>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, costs and effort.</p> <p>This also comes at a cost of stability to the infrastructure and quality of service already being delivered.</p>

7.3 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.

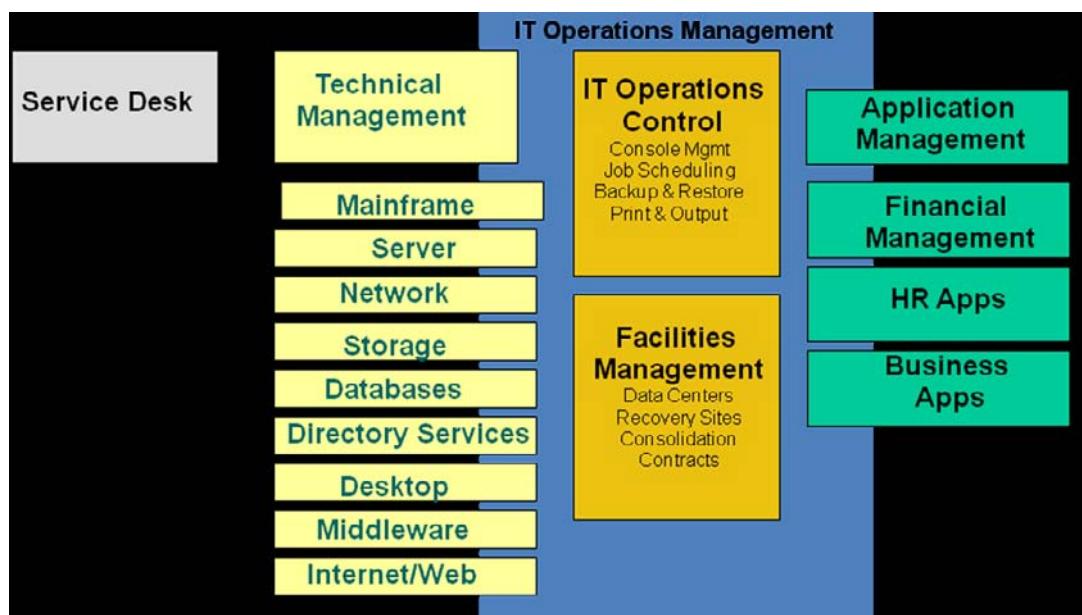


Figure 7.C – The ITIL® Functions from Service Operation

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.

7.3.1 The Service Desk

GOAL: To support the agreed IT service provision by ensuring the accessibility and availability of the IT organization and by performing various supporting activities.

<i>Terminology</i>	<i>Explanation</i>
SERVICE DESK TYPES:	<ul style="list-style-type: none">• Relates to the skill level and first-time resolution rate for service calls.
Call Centre:	<ul style="list-style-type: none">• Handling/logging of large volumes of calls. Low first-time resolution rate for calls and requests.
Help Desk:	<ul style="list-style-type: none">• Manage and co-ordinate incidents. Medium first-time resolution rate for calls and requests.
Service Desk:	<ul style="list-style-type: none">• A wide variety of services offered. High first-time resolution rate for calls and requests.
SERVICE DESK STRUCTURES:	<ul style="list-style-type: none">• Relates to the physical organization of the service desk.
Local:	<ul style="list-style-type: none">• The Service Desk is situated in the same physical location (or time zone for international organizations) as the user groups that it serves.
Central:	<ul style="list-style-type: none">• A centralized Service Desk serves multiple user groups from different physical locations.
Virtual:	<ul style="list-style-type: none">• A Service Desk that has no physical structure, but instead relies on technology to coordinate call resolution across disparate Service Desk staff and to provide a centralized Knowledgebase.
Follow-the-Sun:	<ul style="list-style-type: none">• Utilizing multiple Service Desks across different time-zones in order to provide 24x7 availability of the Service Desk. Typically there will still be a centrally managed Knowledgebase to enhance the quality of support delivered.

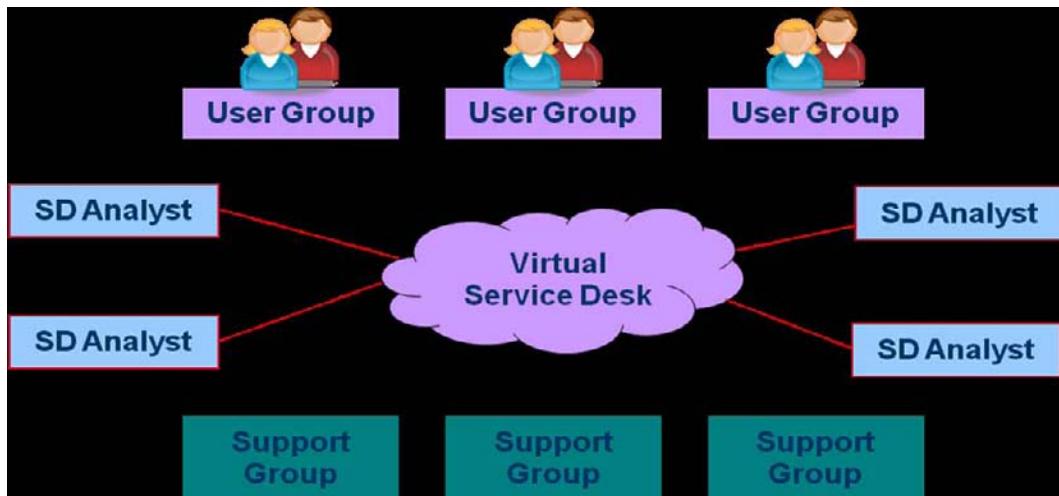


Figure 7.D – A Virtual Service Desk structure

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 are 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.

Self-Help

Many organizations find it beneficial to offer “Self Help” capabilities to their users. The technology should therefore support this capability with some form of web front-end allowing web pages to be defined offering 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 online the status of their parcels 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.

Key Performance Indicators for the Service Desk

It is important to use a balanced range of metrics for measuring the effectiveness and efficiency of the Service Desk. Typical metrics include:

- Number of calls to Service Desk;
- Number of calls to other support staff (look to decrease escalations over time);
- Call resolution time;
- Customer satisfaction (surveys);
- Use of self help (where exists).

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
- Promote 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)

7.3.2 Technical Management

Goal: 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 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.

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.

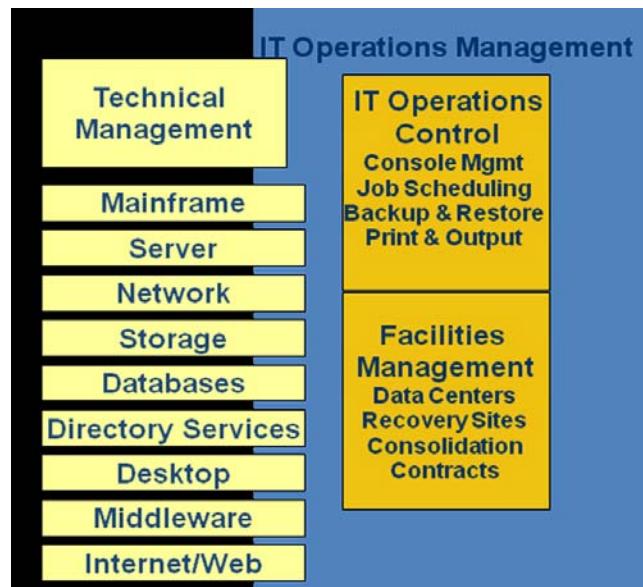


Figure 7.E – Technical Management

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.F – Staff making up the Technical Management Function

It is important that the Technical Management function is made up of both the support staff as well as those involved in the design of the service. This is because quality support needs the input of the design team, and quality design needs input from those who will be supporting the service.

7.3.3 IT Operations Management

Goal: To perform the daily operational activities needed to manage the IT Infrastructure. This is done according to the performance standards defined during Service Design.

In many senses, the function performs many of the logistical activities required for the effective and efficient delivery and support of services (e.g. Event Management).

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.

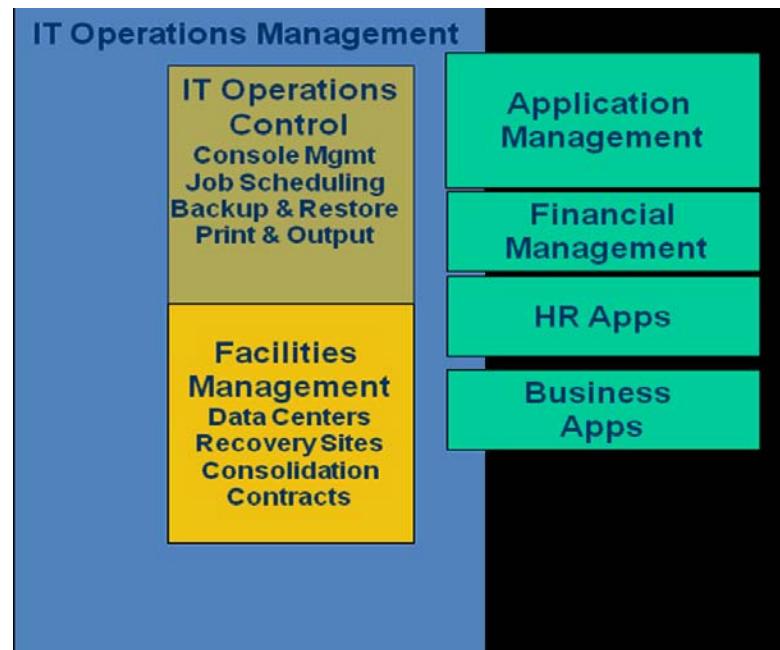


Figure 7.F1 – IT Operations Management

Roles and Responsibilities:

- Maintenance of the 'status quo' to achieve stability of the organization's day to day processes and activities.
- Regular scrutiny and improvements to achieve improved service at reduced costs, whilst maintaining stability.
- Swift application of operational skills to diagnose and resolve any IT operations failures that occur.

IT Operations Management has two unique functions, which are usually organized into two groups:

1. IT Operations Control

Generally staffed by shifts of operators and ensures that routine operational tasks are carried out. Also provides centralized monitoring and control activities, usually using an *Operations Bridge* or *Network Operations Centre*. *Event Management* is a process carried out by IT Operations Control.

2. Facilities Management

Management of the physical IT environment, usually data centers or computer rooms. In some organizations many physical components have been outsourced and Facilities Management may include the management of the outsourcing contracts.

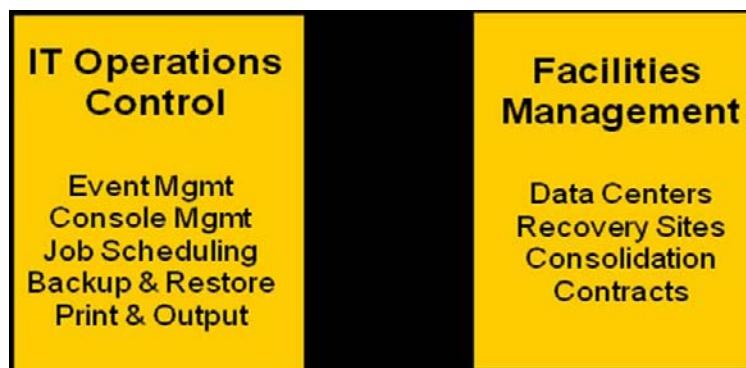


Figure 7.G – Two sub-groups of IT Operations Management

7.3.4 Application Management

Goal: To help design, implement and maintain stable applications to support the organization's business processes.

Application Management is usually divided into departments based on the application portfolio of the organization allowing easier specialization and more focused support.

Roles and Responsibilities:

- Managing Applications throughout their lifecycle;
- Supports and maintains operational applications, and plays an important role in design, testing and improvement of applications that form part of IT Services;
- Support the organization's business processes by helping to identify functional and manageability requirements for application software;
- Assisting in the decision whether to build or buy an application;
- Assist in the design and/or deployment of those applications;
- Provide ongoing support and improvement of those applications;
- Identify skills required to support the applications.



Figure 7.H – Application Management

7.4 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

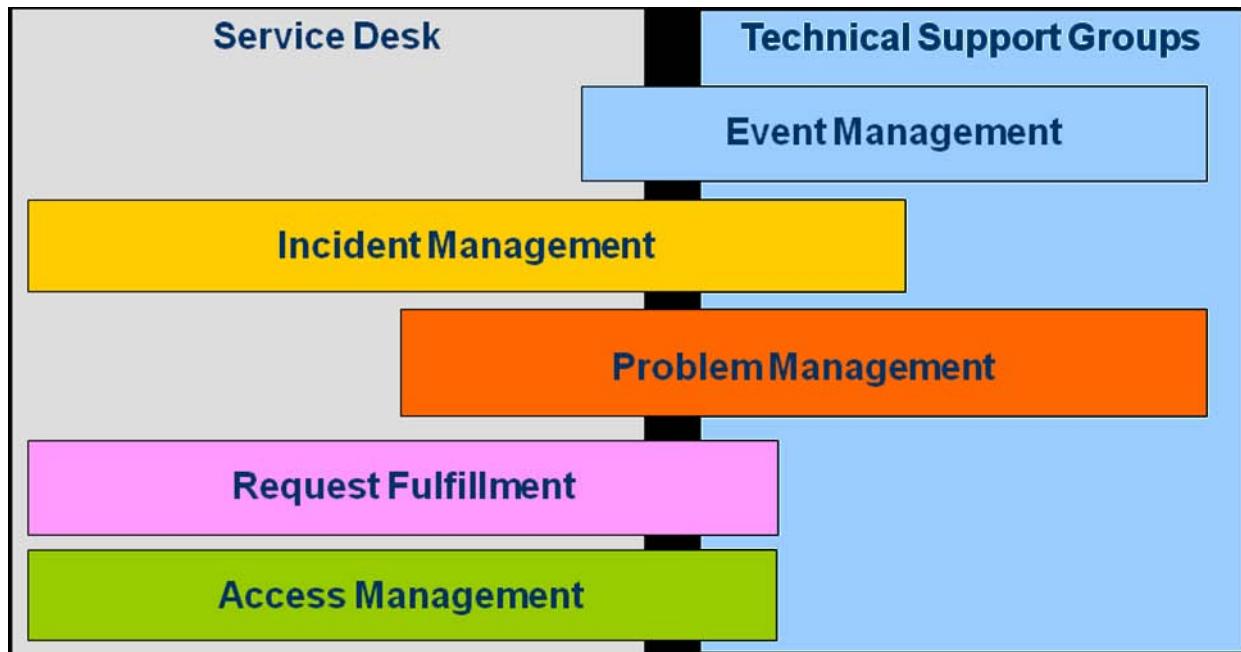


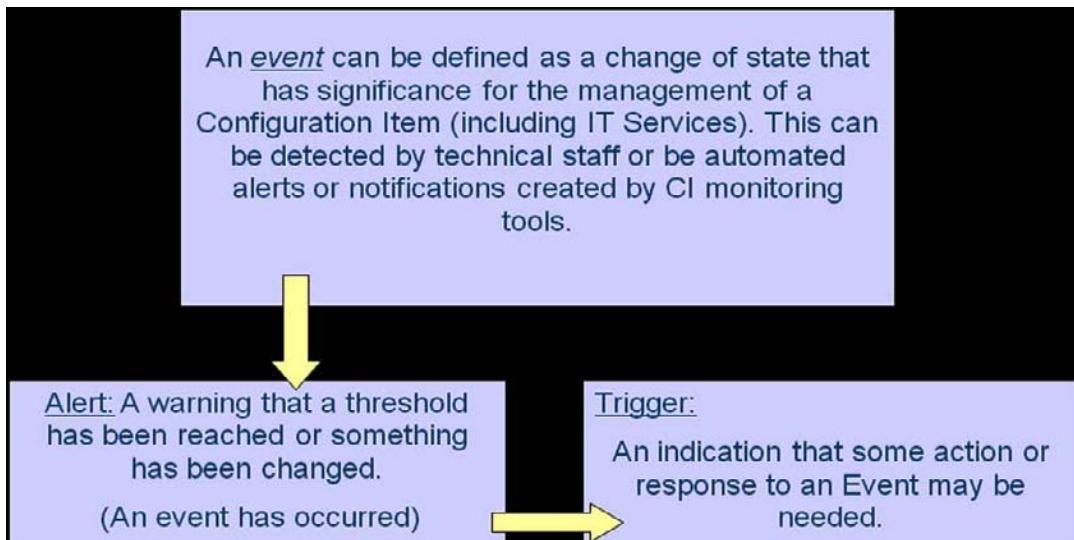
Figure 7.I – Where the Service Operation Processes get carried out

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.

7.4.1 Event Management

Goal: The goal of Event Management is to provide the capability to detect events, make sense of them and determine the appropriate control action. Event Management is therefore the basis for Operational Monitoring and Control.

Event Management should be utilized to detect and communicate operational information as well as warnings and exceptions, so that input can be provided for reporting the service achievements and quality levels provided. It may be used for automating routine activities such as backups and batch processing, or dynamic roles for balancing demand for services across multiple infrastructure items/sources to improve performance.



There are many different types of events, for example:

- Events that signify regular operation (e.g. *A scheduled backup occurred successfully*)
- Events that signify an exception (e.g. *A scheduled backup failed*)
- Events that signify unusual but not exceptional operation. These are an indication that the situation may require closer monitoring (e.g. *No backup initiated within last 72 hours*)

Activities

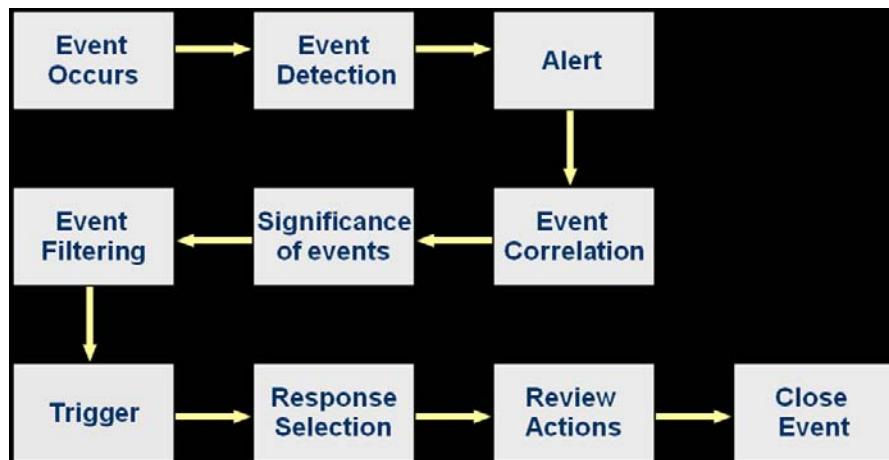


Figure 7.J – Activities of Event Management

NOTE: In most organizations' IT infrastructure there would be a significant amount of events occurring every day, which may impact on the way in which events are correlated and provide triggers indicating a response is needed.

Event Management should be developed over time to any service management process that requires monitoring and control. While initially the focus will be on providing the foundation for service operation with input to Incident and Problem Management, other possible interfaces that are appropriate include:

- Configuration Management, with events providing information on the current (real-time) and historical status of CIs
- Service Design processes such as Information Security, Capacity and Availability Management. Where thresholds have been set in the design of a service and associated components, Event Management should be utilized to generate events and response actions
- Service Level Management, where Event Management can enhance the capabilities to safeguard SLAs and reduce the business impact of any failures as soon as possible.

7.4.2 Incident Management

Goal: To restore normal service operation **as quickly as possible** and minimize the adverse impact on business operations, thus ensuring that the best possible levels of service quality and availability are maintained.

Normal service operation is defined as operating within the agreed Service Level Agreement (SLA) limits.

What is the difference between Incident Management and Problem Management?

QUESTION: If we had our gardens and lawns being affected by 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, and 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.)

This shows the difference between Incident Management and Problem Management. Incident Management is not concerned with the root cause, only addressing the symptoms as quickly as possible.

What is an Incident?

1. An unplanned interruption to an IT service.
2. A reduction in the quality of an IT service.
3. Failure of a CI that has not yet affected service, but could likely disrupt service if left unchecked. This can be raised by internal IT staff.

Major Concepts:

Categorization:

		Urgency		
		High	Med	Low
Impact	High	1	2	3
	Med	2	3	4
	Low	3	4	5

Priority

Figure 7.K – Priority Grid

Categorization is the **unemotional/statistical** aspect of prioritization. It uses the following formula:

$$\text{IMPACT} + \text{URGENCY} = \text{PRIORITY}$$

- **Impact:** Degree to which the user/business is affected
- **Urgency:** Degree to which resolution can be delayed

Escalation:

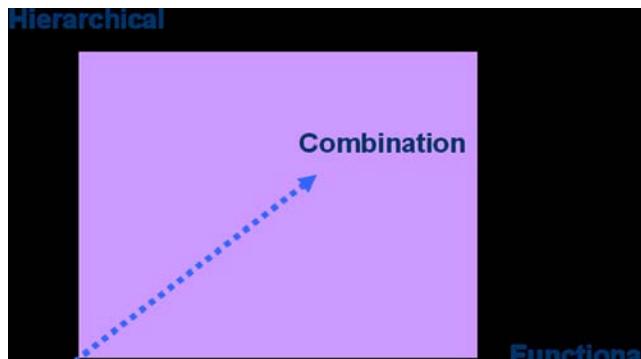


Figure 7.L – Escalation Graph

Escalation is the **human element of Incident Prioritization**. It helps us identify incidents that may need to be moved up or down the priority list due to changing factors or priorities. Escalations can also be combined.

Functional:

- Based on *knowledge or expertise*
- Also known as “Horizontal Escalation”

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

A combination of both escalation methods may also be appropriate.

Activities:

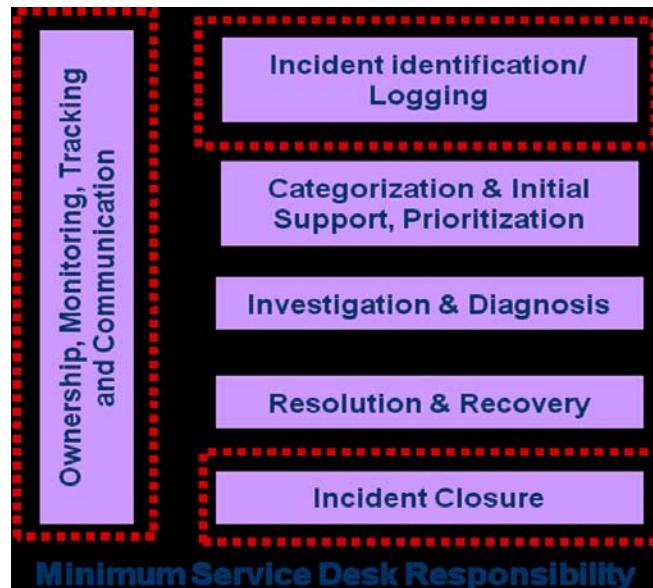


Figure 7.M – Activities of Incident Management

Ownership, Monitoring, Tracking & Communication

- The Service Desk typically OWNS/accountable for ALL Incidents
- Monitor progress, escalation of Incidents
- Advise user and IT management

Incident identification and Logging

- Update/confirm Incident and user details

Categorization, Prioritization (Most critical activity) & Initial Support

- Categorize so the exact type of call is recorded e.g. Incident (E.g. Desktop, Network, Email)
- Assess urgency and impact to assign correct *priority*
- Match against existing Problems/Known Errors
- Match multiple Incidents and create new Problem record (if necessary)
- Provide initial support based on evidence already gathered (such as currently known issues).

Investigation and Diagnosis

- Assess the Incident details and provide workaround (if available)
- Escalate to support areas (Functional) or IT management (Hierarchical)

Resolution and Recovery

- Resolve the Incident or raise a RFC

Incident Closure

- Update details of actions taken and classification of Incident
- Confirm closure with User

Major Incidents:

The highest category or impact defined for an incident. A major incident results in significant disruption to the business.

A separate procedure, with shorter timescales and greater urgency, must be used for 'major' incidents. A definition of what constitutes a major incident must be agreed and ideally mapped on to the overall incident prioritization system – such that they will be dealt with through the major incident process. This often leads directly into Problem Management, to ensure that the root-cause of the Incident is removed and the incident never occurs again.

Roles and Responsibilities:**Incident Manager:**

- Drive effectiveness & 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

Key Performance Indicators for Incident Management:

Just like any other ITIL® process, a balanced range of metrics must be used to demonstrate effectiveness and efficiency of the Incident Management process, including:

- Total number of incidents;
- Percentage of Incidents handled within agreed response time (Incident response-time targets may be specified in SLAs, for example, by impact code);
- Average cost per Incident;
- Percentage of Incidents closed by the Service Desk without reference to other levels of support;
- Number and percentage of Incidents resolved remotely, without the need for a visit.

Challenges affecting Incident Management:

- Are all calls registered? Under a unique number?
- Which priority codes do we use and how is the priority determined?
- Organization of the 1st line
- Organization of the 2nd line, which may be from disparate support groups
- What % “closed on first call” is possible through Incident Management?

7.4.3 Problem Management

Goal: Problem Management is responsible for managing lifecycle of all problems. The primary objectives of Problem Management are:

- To prevent problems and resulting incidents from happening
- To eliminate recurring incidents
- To minimize the impact of incidents that cannot be prevented.

Defined as two major processes:

1. Reactive Problem Management
2. Proactive Problem Management **

** 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.

Terminology	Explanations
Problem:	Unknown underlying cause of one or more Incidents (The investigation)
Known Error:	Known underlying cause. Successful diagnosis of the root cause of a Problem, and workaround or permanent solution has been identified
KEDB:	Known Error Database, where Known Errors and their documented workarounds are maintained. This database is owned by Problem Management.
Workaround:	The pre-defined and documented technique in which to restore functionality to the user with the required functionality. A workaround is NOT a permanent (structural) solution, and only addresses the symptoms of errors. These workarounds are stored in the KEDB (or Service Knowledge Management System).

Relationship with other Processes:

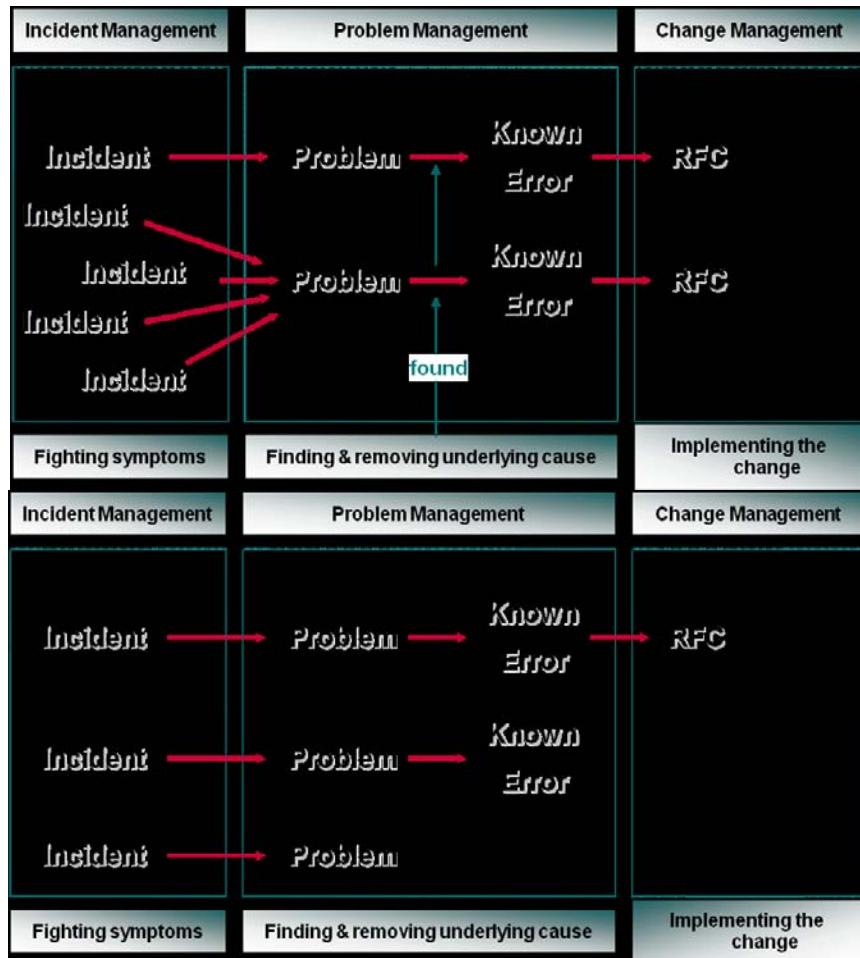


Figure 7.N – Relationships between incidents, problems and known errors

As shown above, the ways in which Problems are identified and corrected occur 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; or
- Because it may be fixed in an upcoming patch from development teams or suppliers

Two Sub-Processes of Problem Management

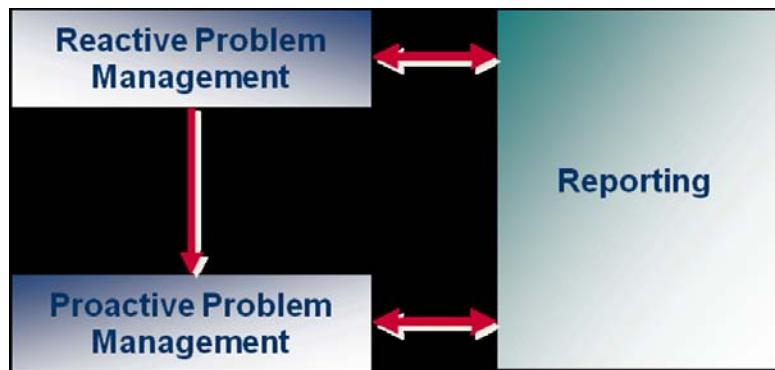


Figure 7.O – The two sub-processes of Problem Management

The activities of Problem Management are carried out within the Proactive and Reactive Problem Management. The main goal of Proactive Problem Management is to identify errors that might otherwise be missed. Proactive Problem Management analyses Incident Records, and uses data collected by other IT Service Management processes and external sources to identify trends or significant problems.

Reactive Problem Management

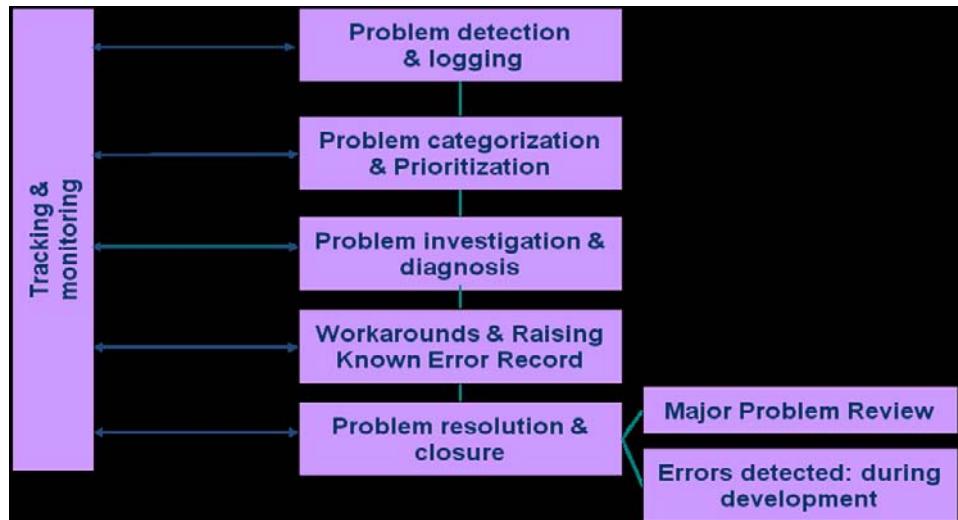


Figure 7.P – The activities of Reactive Problem Management

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
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)

Roles and Responsibilities

Problem Manager

- Drive effectiveness & efficiency of process
- Manage the Problem Management team
- Liaise with customers, IT executive, IT platform managers

Skills

- Business knowledge
- Lateral thinker
- Coordination skills

Problem Management Team

Including Application and Technical Management functions

- Reactive & proactive problem management
- Provide management reports
- Assist Incident Management

Skills

- Analytical, technical, business knowledge

7.4.4 Request Fulfillment

Goal: Request Fulfilment is concerned with fulfilling requests from the end user community using consistent and repeatable methods. The objectives include:

- To provide a channel for users to request and receive standard services for which a pre-defined approval (from Change Management) qualification exists
- To provide information to users and customers about the availability of services and the procedure for obtaining them
- To source and deliver the components of requested standard services
- To assist with general information, complaints or comments

Scope: The scope of Request Fulfilment is influenced heavily by the success of Change Management and what types of pre-approved changes can be effectively managed, controlled and implemented by the IT department. As part of continual improvement, the scope of Request Fulfilment should grow over time as maturity develops for Service Requests, including:

- Users and customers asking questions, providing comments and making complaints
- Users seeking changes to their access levels (utilizes Access Management)
- Users wishing to have common services and applications installed for their use (including Standard Changes)

Many elements of Request Fulfilment may be automated through the use of self-help such as websites and user applications, with manual activities being used where necessary to fulfill the request.

Request Models: As many service requests will be 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) with 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 Fulfilment 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. Fulfilment

The tasks required for Fulfilment 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 Fulfilment should be interfaced with existing procurement and supplier processes; however the Service Desk should maintain control and visibility for all requests regardless 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.

7.4.5 Access Management

Goal: Access Management's primary objective is to provide capabilities for the granting of authorized users the right to use a service while preventing access to non-authorized users. In doing so, it helps to protect the confidentiality, integrity and availability (CIA) of the organization's services, assets, facilities and information. In practice, Access Management is the operational enforcement of the policies defined by Information Security Management.

Relationship with other Processes

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. As described above, the process 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.

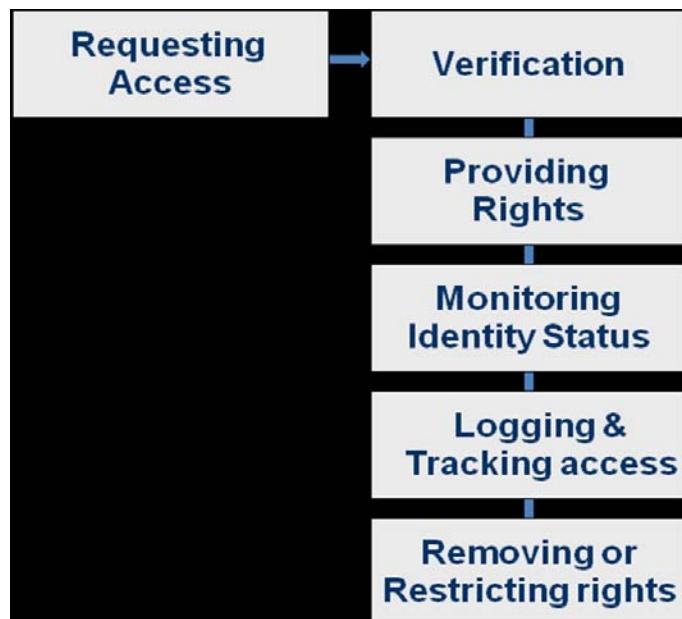


Figure 7.Q – Access Management Activities

Figure 7.Q 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.

7.5 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 phases.

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.

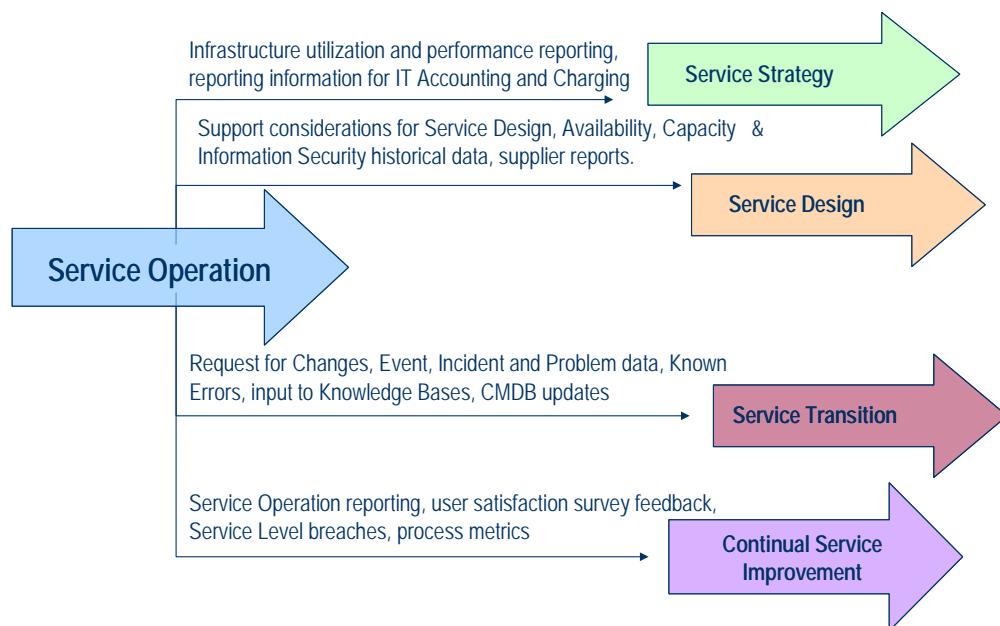


Figure 7.R – Some outputs to other lifecycle phases.

7.6 Service Operation Scenario

7.6.1 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

7.6.2 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.

7.7 Service Operation Review Questions

7.7.1 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

7.7.2 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.

7.7.3 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

7.7.4 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 maximise business impact
- d) Contributing to the reduction of impact

7.7.5 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 web site to download a licensed copy of software from a list of approved options

7.7.6 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

7.7.7 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

7.7.8 Question 8

Which of the following is NOT an objective of Service Operation?

- a) Through 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

7.7.9 Question 9

Which of the following BEST describes the purpose of Event Management?

- a) The ability to detect events, analyse 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

7.7.10 Question 10

Which process or function is responsible for management of the Data centre facility?

- a) IT Operations Control
- b) Supplier Management
- c) Facilities Management
- d) Technical Function

8 Continual Service Improvement



Figure 8.A – Service Design

Processes:

- Service Level Management*
- Service Measurement & Reporting
- Continual Service Improvement (7 Step) Process

*Although Service Level Management primarily fits within the Service Design Phase, it plays a very large part in CSI, and therefore is discussed in this section.

8.1 Objectives

To ensure continual improvements to IT Service Management Processes and IT Services (essentially anything within the scope of IT Service Management).

Continual Service Improvement is the phase that binds all the other elements of the Service Lifecycle together and ensures that both the services and the capabilities for providing them continually improves and matures.

8.2 Major Concepts

The Continual Service Improvement Model

The CSI Model provides the basis by which improvements are made to both services and the capabilities of an IT Service Provider. They are questions asked in order to ensure all the required elements are identified to achieve continual improvement.

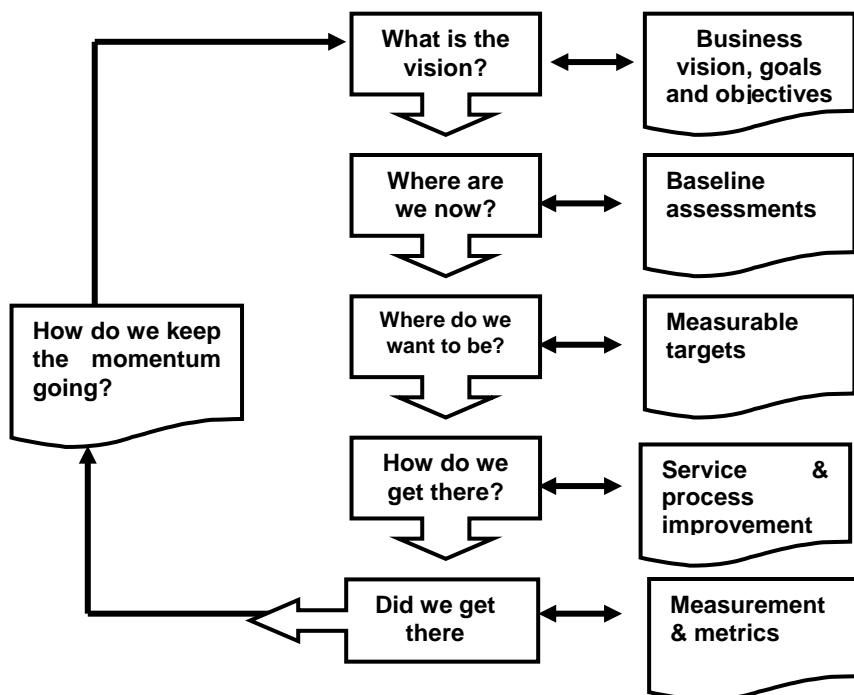


Figure 8.B – Continual Service Improvement Model.
© Crown Copyright 2007 Reproduced under license from OGC

The Continual Service Improvement Model summarizes the constant cycle for improvement. The questions require close interactions with all the other ITIL® processes in order to achieve Continual Service Improvement.

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.

8.3 Continual Service Improvement Processes

8.3.1 Service Level Management

GOAL: The primary goal of Service Level Management is to ensure that an agreed level of IT service is provided for all current IT services, and that future services are delivered to agreed achievable targets. It also proactively seeks and implements improvements to the level of service delivered to customers and users.

Service Level Management is a critical element of Continual Service Improvement. Why embark on any service improvement initiative if the customers and the business are satisfied with the levels of service already received? Because business requirements quickly change!

Activities

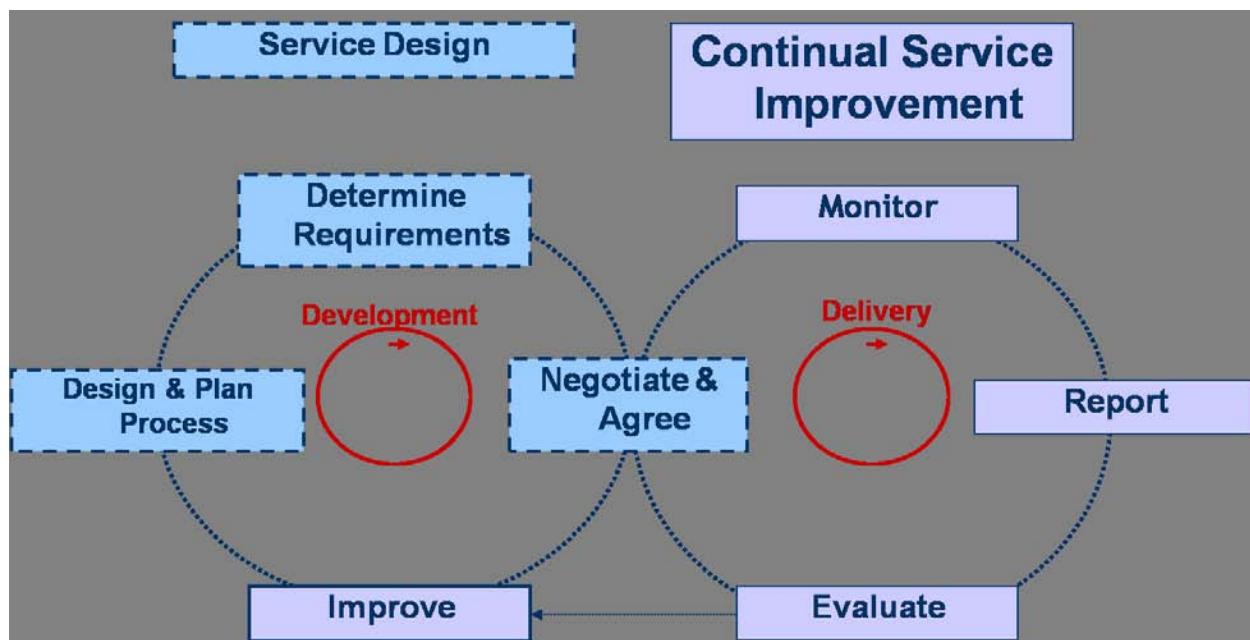


Figure 8.C – The Activities of Service Level Management

Within Continual Service Improvement, Service Level Management is concerned with improving services and processes through constant:

- Analyzing data gathered during Service Operation
- Reporting
- Evaluating
- Improving

The major focus of Service Level Management within Continual Service Improvement is ***identifying potential service improvements.***

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 organization; with *authority* to do what is necessary
- Manages Service Catalogue, SLAs and OLAs and ensures alignment of Underpinning Contracts
- Identifies and manages improvements to services and processes
- Analyses and reports on Service Level Achievements

Skills

- Relationship Management
- Patience, tolerance, resilience
- An understanding of the customer's business and how IT contributes to the delivery of that product or service

Challenges Affecting Service Level Management:

- Monitoring of pre-SLA achievements, where to begin?
- Identifying targets that are achievable and reasonable
- Insufficient focus, resources and time
- Inadequate seniority of SLM staff
- Underpinning contracts ignored
- SLAs too long, written in technical jargon and not customer focused
- Improvement actions not adhered to

Key Performance Indicators of Service Level Management

Statistics:

- Number/Percentage of services covered by SLAs
- Number/Percentage SLAs supported by UCs & OLAs
- Number/Percentage of service targets being met

Yes / Why Questions:

- Are service level achievements improving?
- Are customer perception statistics improving?
- Are IT costs for service provisions decreasing for services with stable (acceptable but not improving) Service Level Achievements?

Implementing effective and efficient Service Level Management should produce a “Yes” answer to each of the above questions.

If the answer is No...

If the answer is “No” to any of these questions

- The very next question that should be asked is “Why?”

From this we can investigate where the process is deficient and begin a plan for improvement. Communicating this to the business also gives them a better understanding of the complexity of providing the services and more importantly allows the business to be actively involved with assessing the costs, risks and plausibility of what will be needed in order to bridge the gap.

8.3.2 Service Measurement and Reporting

GOAL: To coordinate the design of metrics, data collection and reporting activities from the other processes and functions.

There are four main reasons to monitor and measure:

1. **Validate:** Are we supporting the strategy and vision?
2. **Direct:** Based on factual data, people can be guided to change behavior
3. **Justify:** Do we have the right targets and metrics?
4. **Intervene:** Take corrective actions such as identifying improvement opportunities

Measurement of all the process metrics takes place throughout all the Lifecycle phases. CSI uses the results of these measurements to identify and establish improvements via reports.

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 KPIs and activity metrics for the service management processes which determine the overall health of a process. Four key questions KPIs can help 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 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.

Baselines: A benchmark captured and used as a reference point for later comparison.

It is important that baselines as documents are recognized and accepted throughout the organization. Baseline must be established at each level: strategic goals, and objectives, tactical process maturity and operational metrics and KPIs.

Examples

1. A Service Level Achievement Baseline can be used 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.

8.3.3 CSI (7 Step) Improvement Process

GOAL: To coordinate a structured approach for improvements to IT services and ITSM processes.

The Deming Cycle: A foundation for continual improvement

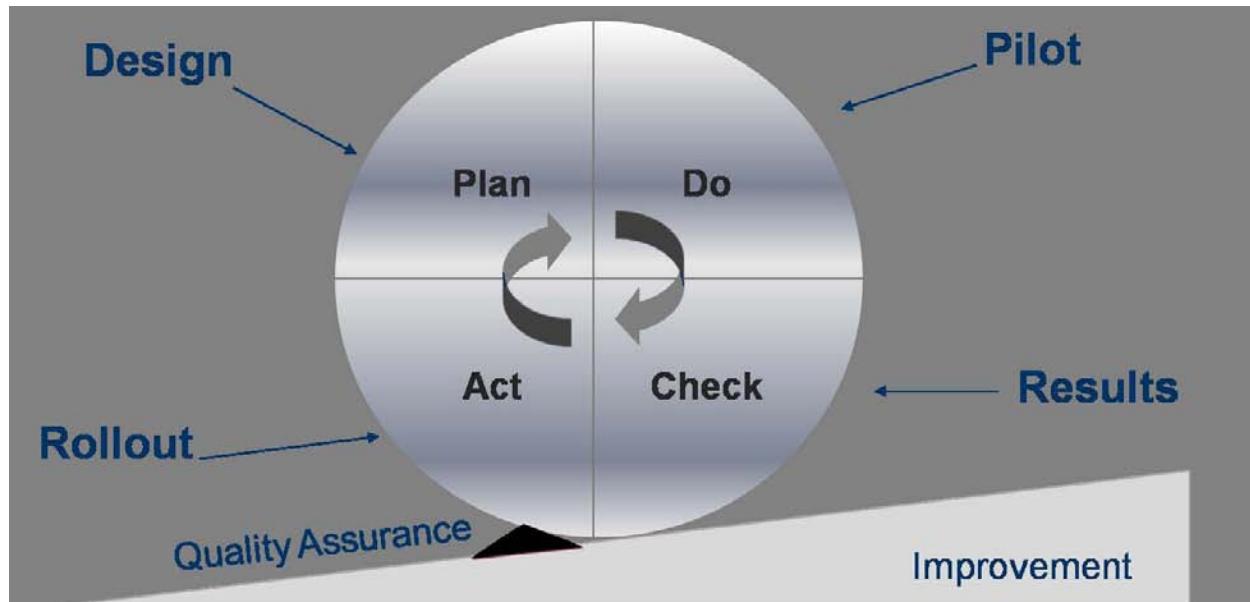


Figure 8.D – The Deming Cycle

Continuous improvement is a part of every process in ITIL®. The CSI Improvement Process is based on the Deming Cycle of Continual Improvement (Plan, Do, Check, Act).

Implementing ITIL®/ITSM is an ongoing activity, where you improve quality through incremental steps. These four steps are carried out *in the exact order, as many times as necessary* in order to achieve the improvement desired.

Some of the items that occur during each of the 4 phases:

- **Plan:** Scope, requirements, objectives, Roles and Responsibilities
- **Do:** Funds, Policies, reports, managing, changing
- **Check:** Monitor against plans, survey, report
- **Act:** Policy on improvement, assessment, implementation (if appropriate)

Notes on William Edwards Deming:

An American statistician best known for his work in Japan in the post-WWII period. There, from 1950 onward he taught top management how to improve design (and thus service), product quality, testing and sales (the last through global markets). Deming made a significant contribution to Japan's later renown for innovative high-quality products and its economic power.



Figure 8.E – The CSI (7 Step) Improvement Process

The Deming Cycle is transformed into more detailed steps and actions to be taken for the improvement of IT services and IT Service Management processes. Like the Deming Cycle, these steps need to be taken in sequential order, as many times as necessary to drive the improvement desired.

8.4 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 phase:

- 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.

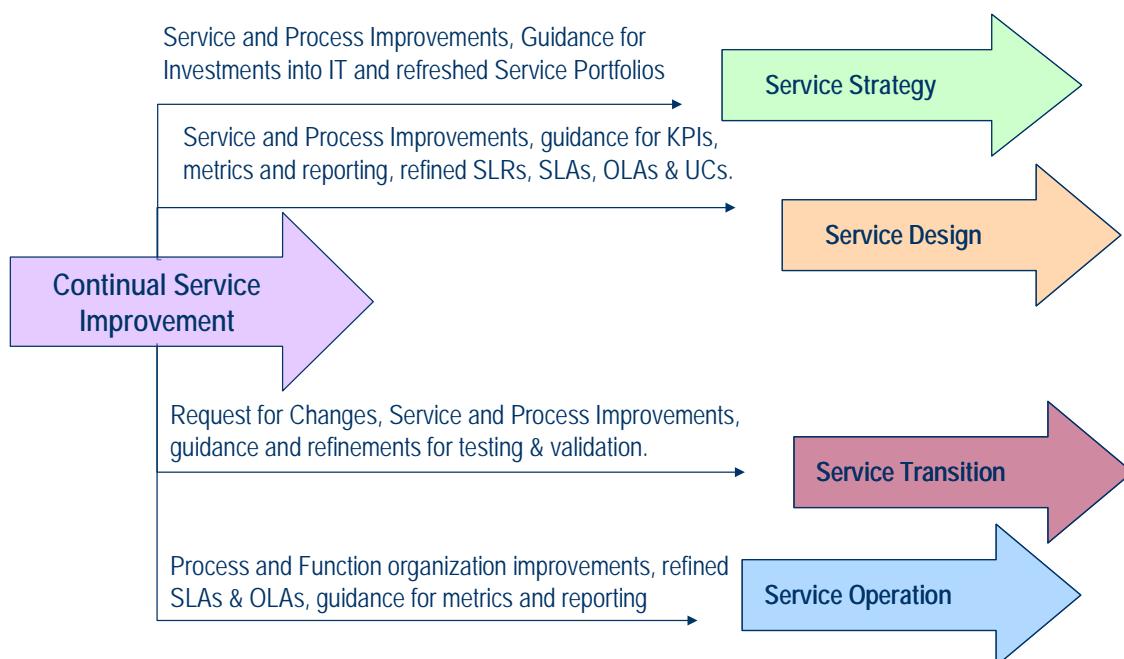


Figure 8.F – Some outputs to other lifecycle phases.

8.5 Continual Service Improvement Scenario

8.5.1 Service Level Management

SLM will be constantly reviewing the SLA and achievements to see if targets are being met. For example – it was found that the availability of the service dropped to 80%. This combined with the increase in the use of the HYPE service; it was decided to implement a Service Improvement Plan (SIP) to identify how this service can be improved.

8.5.2 Service Measurement and Reporting

To do this effectively, it was necessary to take metrics and data and analyze against targets.

8.5.3 CSI Process

The CSI improvement model was used as a roadmap for this SIP. As the business needs changed, so had their 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... at a cost, of course.

This will identify:

- Technology improvements
- Process improvements
- Document improvements
- Training etc.

And so it continues!

8.6 Continual Service Improvement Review Questions

8.6.1 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, analyse, direct and improve

8.6.2 Question 2

Which is the first activity of the Continual Service Improvement (CSI) model?

- 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

8.6.3 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

8.6.4 Question 4

Which of the following is NOT a step in the Continual Service Improvement (CSI) model?

- a) What is the vision?
- b) Did we get there?
- c) Who will help us get there?
- d) Where are we now?

8.6.5 Question 5

What is the CORRECT order of the first four activities in the 7 Step Improvement Process?

- a) Define what you should measure, define what you can measure, gather data and process data
- b) Plan, Do, Check, Act
- c) What is the vision, where are we now, where do we want to be, how do we get there?
- d) Gather data, process data, analyse data, present data

9 ITIL® Foundation Exam Tips

9.1 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

9.2 Practical Suggestions

- Read the question CAREFULLY
- At this level of exam 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”
- 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!

10 Answers to Review Questions

10.1 Service Strategy

1C; 2A; 3A; 4C; 5B; 6A; 7D; 8B; 9B; 10D

10.2 Service Design

1B; 2A; 3D; 4D; 5B; 6B; 7A; 8B; 9C; 10D

10.3 Service Transition

1C; 2B; 3D; 3B; 5B; 6C; 7A; 8B; 9A; 10B

10.4 Service Operation

1C; 2A; 3B; 4D; 5B; 6B; 7C; 8A; 9A; 10C

10.5 Continual Service Improvement

1B; 2B; 3B; 4C; 5A

11 Glossary

Alert: A warning that a threshold has been reached, something has changed, or a failure has occurred.

Asset: Any resource or capability.

Application Sizing: Determines the hardware or network capacity to support new or modified applications and the predicted workload.

Baselines: A benchmark used as a reference point for later comparison.

CMDB: Configuration Management Database

CMS: Configuration Management System

Configuration Item (CI): Any component that needs to be managed in order to deliver an IT Service.

DML: Definitive Media Library

Function: A team or group of people and the tools they use to carry out one or more processes or activities.

Incident: An unplanned interruption to, or reduction in the quality of, an IT service

Known Error: A problem that has a documented Root Cause and a Workaround

KEDB: Known Error Database

Maintainability: A measure of how quickly and effectively a CI or IT service can be restored to normal after a failure.

Modeling: A technique used to predict the future behavior of a system, process, CI etc

MTBF: Mean Time Between Failures (Uptime)

MTBSI: Mean Time Between Service Incidents

MTRS: Mean Time to Restore Service (Downtime)

OLA: Operational Level Agreement – internal agreements that support SLAs.

Process: A structured set of activities designed to accomplish a specific objective.

Process Owner: Role responsible for ensuring that a process is fit for purpose.

Remediation: Recovery to a known state after a failed Change or Release

RFC: Request for Change

Service: A means of delivering value to Customers by facilitating Outcomes Customers want to achieve without the ownership of specific Costs and risks

Service Owner: Role that is accountable for the delivery of a specific IT service

SCD: Supplier and Contracts Database

Service Assets: Any capability or resource of a service provider

Serviceability: Measures Availability, Reliability, Maintainability of IT services/CI's under control of external suppliers.

SIP: Service Improvement Plan

SKMS: Service Knowledge Management System

SLA: Service Level Agreement – agreements between service providers and customers.

SLM: Service Level Manager

SLR: Service Level Requirements

SSIP: Supplier Service Improvement Plan

Status Accounting: Reporting of all current and historical data about each CI throughout its lifecycle.

Trigger: An indication that some action or response to an event may be needed. All processes are triggered by some event or action taking place; otherwise we would not know when to execute them.

Tuning: Used by Capacity Management to identify areas of the IT infrastructure that could be better utilized.

UC: Underpinning Contract – manages supplier relationships and services provided by them.

Utility: Functionality offered by a product or service to meet a particular need. Often summarized as ‘what it does’.

VBF: Vital Business Function

Warranty: A promise or guarantee that a product or service will meet its agreed requirements.

Workaround: The pre-defined and documented technique in which to restore functionality to the user with the required functionality. A workaround is NOT a permanent (structural) solution, and only addresses the symptoms of errors.

12 Certification

12.1 ITIL® Certification Pathways

There are many pathway options that are available to you 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.

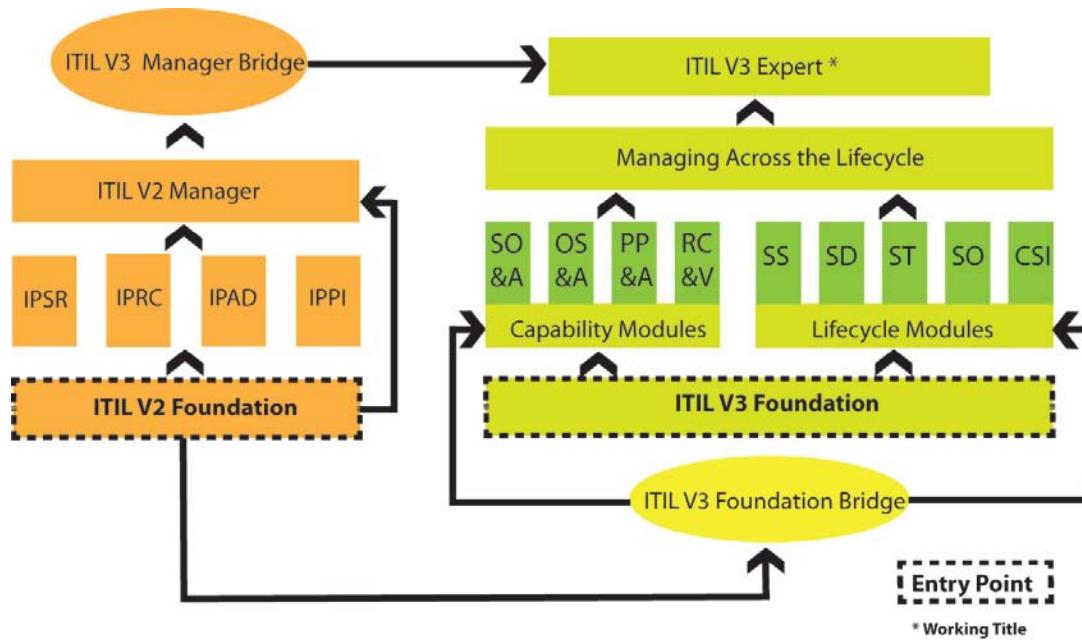


Figure 12.A – ITIL® Certification Pathway

For more information on certification and available programs please visit our website
<http://theartofservice.com>.

12.2 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 itself and issues relating to earning actual standards compliance.

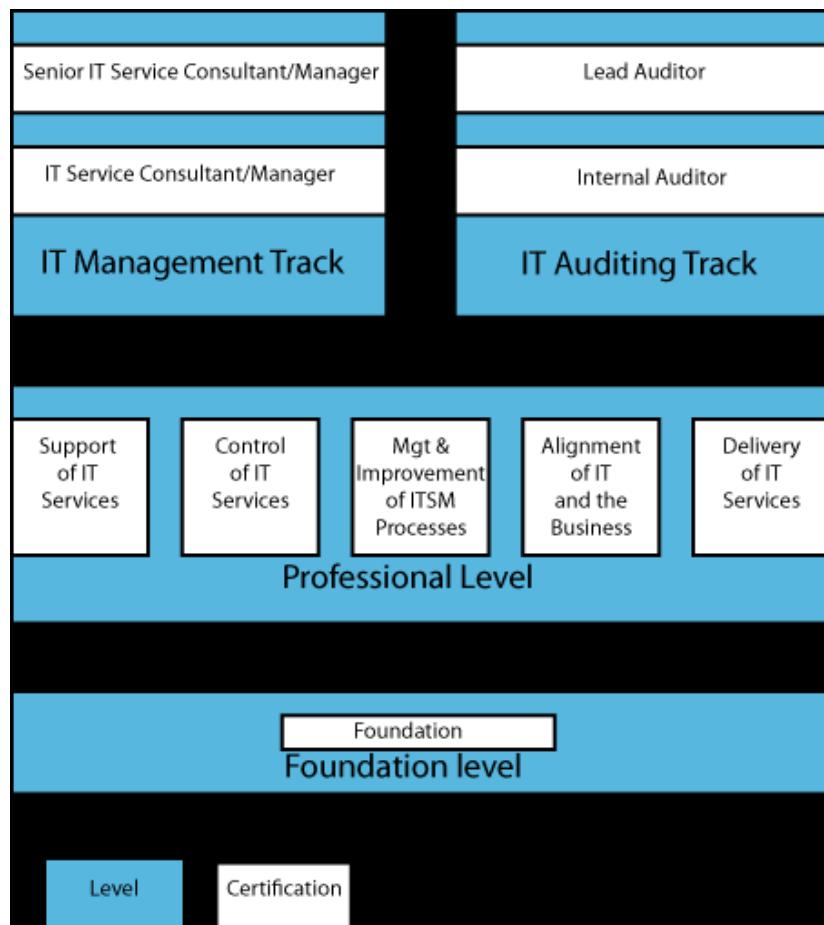


Figure 12.B – ISO/IEC 20000 Certification Pathway

For more information on certification and available programs please visit our website
<http://theartofservice.com>.

13 INDEX

A

ability 11-12, 40, 42, 67, 80, 87, 120, 146
service provider's 85, 109
acceptance criteria, Service 48
Access Management 4, 140, 142, 144
account 6, 34-5
accountability 18
act 156, 160
activities, technical 8
Activities of Incident Management 132
Activities of Information Security Management 77-8
Activities of Service Level Management 50, 151
Activity-based Demand Management 38
agreements 51-2, 55, 59, 63, 73, 164
alignment 3, 7-8, 152
answers 19, 29, 52, 99, 153, 161-2
ANSWERS 4, 162
answers, correct 161
Applicable service hours 54
Application Management 4, 12, 122, 126, 144
Application Service Provision 57
applications 12, 14, 18, 32, 55, 87, 95, 106, 126, 140, 146
approach
 holistic 47, 158
 push 104
approval, financial 99, 141
assemblies 102
assets 12, 34, 71-2, 93, 142
 strategic 12, 15, 25
attributes 3, 6, 34, 41, 89, 91, 110
 required service 40
audits 75, 90, 92, 111
availability 19-20, 23, 27, 38, 41-2, 66-7, 70, 75, 82-3, 119, 130, 142-3, 154, 159
Availability and Capacity Management 139
Availability Management 3, 8, 44, 66, 68, 70, 81-2, 129, 142, 144
 Capacity Management 49
Availability Management and Incident Management 68
Availability Management Process 13
Availability Manager 70
Average time 69

B

back-of-house, processes 127
backups 53, 128, 144
 scheduled 128
balance 33, 36, 78, 99, 115-17
balanced scorecard 44-5
bang 103-4, 111
Base Service Package 45
baselines 63, 65, 112, 150, 154-5, 163
batch jobs 39

batch processing 128
batch processing jobs 146
BCM (Business Continuity Management) 71-2
benefits 7, 13, 27, 34, 37, 40, 85-6, 92, 99, 109, 136, 143, 158
BIA (Business Impact Analysis) 71-2
budgets 6, 23, 36, 40-1, 59, 65, 85, 109
business 5, 7-8, 13, 32, 34-7, 42-3, 49-50, 55, 59, 66-8, 70-1, 80-1, 85-6, 116, 145-6, 158-60 [12]
 articulate 30
 changing 47-8, 115-16
 customer's 152
business action 13
business activity 37
 patterns of 38
Business and Technical Service Catalogues 60
business approval 141
business areas 96
business benefits, expected 99
Business Capacity Management 63, 65
Business Case 13
Business Continuity Management 71
Business Continuity Management: (BCM) 71-2
Business Continuity Strategy 72
Business Desires/Opportunities 34
business expertise 56
business focus 116
Business Function 31, 67, 71, 165
business impact 44, 129
 bottle-necks 101
 maximise 145
Business Impact Analysis (BIA) 71-2
business knowledge 139
business operations 68, 130
business/organization 105
business outcomes 40
Business Plan 65
business plans/goals 159
Business Process Outsourcing 56
business processes 8, 27, 38, 51, 56, 61, 67, 71-2, 85, 90, 142
 efficient 13
 enhancing 29
business requirements 63, 65, 70, 79, 108, 151
 high-level 108
 ignoring changing 116
 meeting 116
business security 75
Business Service Catalogue 61
business strategy 20, 117
business support 107
business terminology 61
business time scales 71
business understanding 133
business units 13, 61, 88
business users 115
business value 29-30
business vision 150
businesses change, associated 33

C

CAB (Change Advisory Board) 96, 98, 100-1, 110, 113
Calculated 69
calls 42, 102, 119-20, 132, 134
 Number of 121
 Service Desk 107
capabilities 5, 12, 25-6, 29, 31, 34, 36, 48, 55, 62, 85, 115, 120, 128-9, 149-50, 163-4 [1]
capacity 19-20, 26-7, 37-9, 42, 62-3, 65, 107-8, 143
Capacity and Availability Management 129
Capacity Management 3, 8, 37, 44, 62, 64-5, 82, 139, 165
Capacity Management process 82
Capacity Manager 65
Capacity Plan, services 65
Categorization 131-2
certification 4, 167-8
Certification Pathway 4, 167-8
Challenges Affecting Service Level Management 152
Change Advisory Board 96
Change Advisory Board, see CAB
Change Management 4, 73, 90, 94-5, 97-9, 101, 103, 106, 110, 112-13, 136, 140-1, 145
Change Management and Service Validation 38
change management process 96, 98, 101
Change Manager 96, 98-101
Change Models 95, 98, 140
change proposal 97
changed services 47-8, 82, 85, 103-4, 106-7
Charge business 43
Chargeback 35
Charging customers 35
Chief Information Officer 33
choice 27-8, 161
CI (Configuration Item) 12, 18, 57, 60-1, 69, 79, 83, 89-90, 92-3, 95-6, 109-11, 130, 145, 163-4
CIs (Configuration Items) 57, 60-1, 83, 89-94, 101, 103, 110-11, 129, 145, 163
CIs 89, 91
classification, Incident 133
closure 133, 141
CMDB (Configuration Management Database) 88, 90, 92, 95, 102-3, 109, 121, 163
CMDB updates Service Operation 143
CMS (Configuration Management System) 57, 60-1, 88, 90, 97, 163
Commercial Confectionery Organizations 37
communication 16, 26, 35, 59, 61, 74, 133
complexity 28, 49, 57, 60, 153
Component Capacity Management 63, 65
components 14, 28, 60-1, 63, 65, 67, 69, 80, 86, 88-90, 102, 110, 116, 139-40, 154, 163
 physical 16, 125
components 70
concepts 3-4, 6-7, 11, 14, 19, 21-2, 26, 48, 87, 107-8, 116, 131, 150
confidentiality 75, 142
configuration data, service provider's 88
Configuration Item, see CI
Configuration Item information 79, 109
Configuration Items, see CIs
Configuration Management 4, 40, 89, 93-4, 101, 112, 155
 sound Service Asset & 91
 Service Asset & 85
Configuration Management Database, see CMDB
Configuration Management System, see CMS

conflict 54, 115-16
consistency 56-7, 60, 103-4, 117
constraints 26-7, 107
 business processes, Time 72
 services, Time 72
continual improvement 6, 13, 140, 149-50, 156
Continual Service Improvement 4, 21-3, 41, 49, 58, 79, 109, 135, 143, 149-52, 158, 160, 162
Continual Service Improvement Chapter 54
Continual Service Improvement Model 150
Continual Service Improvement Processes 4, 151
Continual Service Improvement Review Questions 4, 160
Continual Service Improvement Scenario 4, 159
Continual Service Improvement Summary 4, 158
continuity 19-20, 28, 42, 72-5
continuity strategies 71, 73
Continuous Service Improvement, see CSI
Contract Database 55, 57
contract management 57-8, 83
contracts 51-2, 55, 57-8, 108, 152
control 35, 48, 67, 77, 90-2, 111, 128-9, 141, 146, 164
cook 14
coordinates 23, 100, 105, 154, 156
CORE Business Processes 8
Core Service Package 27-8, 42, 44-5
Corporate/Business decisions 74
cost elements 35-6
Cost of Service 117
cost types 35
Cost Units 36, 41
costs 12-15, 25, 28, 34-7, 40, 57, 80, 85, 89, 99, 117, 122, 136, 138, 141, 153 [2]
 improved quality service provision 7
 reduced 92, 124
 variation of 85, 109
Creating Service Value 26
Crown Copyright 11, 16, 19, 26, 38, 55, 60, 72, 87, 93, 97, 100, 108, 150
CSI (Continuous Service Improvement) 4, 23, 41, 149-50, 154, 156-7, 160
CSI Improvement Process 21, 156
CSI Process 159
culture, organizational 25
customer assets 40
Customer/Business Requirements 108
customer enquiries 15
customer experience 14
customer groups 30
customer organizations 57
customer perception statistics 153
customer perspective 36
customer representatives, user 101
customer service skills 14
customer viewpoint 143
customers 5-7, 11-12, 14-16, 19-20, 23, 26-30, 35, 43-4, 49-54, 59-62, 81-2, 84-5, 107-8, 115-17, 138-40, 151-2 [7]
 external 13
 multiple 36
 organization's 34
 outcomes 12, 14, 164
 right 62
 single 36
customers 28, 51

customer's business activity 38

D

damage 72, 77
danger 71, 116-17
databases 30, 87-8, 92, 135
decisions 16, 37, 80, 82, 87-8, 97, 110, 115, 126, 143
Defining Processes 3, 15
Definitive Media Library, see DML
Definitive Spares (DS) 102-3
Degree 131
delivery 5, 13, 17, 61, 104, 115, 127, 152, 164
delivery service 26
Demand Management 3, 36-9, 64, 82
Demand Management techniques 37, 39
Deming Cycle 156-7, 160
departments 49, 53, 118, 122, 126, 140-1
dependencies 59-60, 82, 89
deploy 101-2, 110
deploy processes 105
Deploy Service Management Capability 105
deployment 30, 59, 65, 102-3, 126, 143
Deployment Management 4, 97, 102-3, 112
Deployment Management, Service Validation 85
design 6, 16-17, 19, 23, 25, 31, 37-8, 43, 45, 47-50, 56, 67, 80, 104, 122-3, 126 [7]
design phase, Service 23
Design Service Release 108
Design Service Solution 108
Detailed Service Package Example 28
details 61, 89, 102
detection 69, 78, 92
diagnosis 69, 132, 135, 138
difference 37, 130, 145, 158
disaster 71, 73-4
Disaster 73
disparate Service Desk staff 119
DML (Definitive Media Library) 102-3, 112, 163
downtime 68-9, 164
DS (Definitive Spares) 102-3

E

ECAB (Emergency CAB:) 96, 98
Effective Service Performance 79
Effective Service Transition 85, 109
effectiveness 57, 61, 70, 89, 101, 106, 115, 121, 127, 133-4, 139
effort 7, 14-15, 40, 67, 89, 117
 duplication of 53-4
Emergency CAB: (ECAB) 96, 98
end-to-end business, integrated 47
end-users 11, 97, 120, 133
enterprise information resources 76
environment 17, 92, 95, 118, 125
errors 107, 136-7, 145
escalations 54, 72, 121, 131-2
evaluation 40, 70, 78, 97, 112
Event Management 4, 124-5, 128-9, 144, 146
events 18, 23, 38, 67, 128-9, 143, 146, 165
evolutions 9

exam 161
Expanded Incident Lifecycle 68-9
External Business View 116
External Service Providers 13

F

facilities 72, 142
Facilities Management 125, 147
facts, discrete 86-7
failures 18, 68-9, 75, 107, 129-30, 139, 163
faults 69
Financial Management 3, 8, 34-6, 44, 82, 150
Financial Management & Service Portfolio Management 39
financial resources 34
fit 13, 15, 21-2, 26-7, 42, 45, 107, 164
focus 7-8, 14, 19, 54, 56, 71, 76, 129, 152
 extreme 116-17
focus of ITIL 8, 19
Forced 111
forecast 64-5
Formal arrangements 56
Forward Schedule of Changes (FSC) 65, 109, 112
Foundation Certification 167-8
Foundation Complete Certification Kit Activities 64, 91, 129, 132, 141
Foundation Complete Certification Kit Components 88
Foundation Complete Certification Kit Figure 52, 87, 103, 106, 120, 123
Foundation Complete Certification Kit Financial Management 43
Foundation Complete Certification Kit Important Steps 98
Foundation Complete Certification Kit Incident Closure 133
Foundation Complete Certification Kit Key Performance 134, 153
Foundation Complete Certification Kit Lifecycle 69
Foundation Complete Certification Kit Notes 157
Foundation Complete Certification Kit Overview of Reactive Problem Management activities 138
Foundation Complete Certification Kit Question 45, 83-4, 112-13, 146-7
Foundation Complete Certification Kit Relationship 100, 136
Foundation Complete Certification Kit Roles and Responsibilities 70, 78
Foundation Complete Certification Kit Service Catalogue 81
Foundation Complete Certification Kit Service Retirement 33
Foundation Complete Certification Kit Sub-Processes of Capacity Management 63
Foundation Complete Certification Kit Trigger 165
framework 5, 9, 11, 19, 52
FSC (Forward Schedule of Changes) 65, 109, 112
FSC for Service Desk 100
Fulfilment 141
function organization improvements 158
functionality, overlapping business 32
functions 3, 12, 17-18, 21-2, 45, 56, 112, 118, 124, 143-4, 147, 154, 163

G

Generic Process Elements 16
goal 5, 7, 29, 31, 34, 54, 107, 117-18, 122, 124, 126-8, 130, 135, 137, 140, 142 [1]
groups 12, 39, 50, 95-6, 98, 124, 163
growth, support business 25
guidance 18, 20-1, 25, 48, 109, 115, 158

H

hardware 6, 14, 28, 35, 43, 64, 71, 91, 101-2, 163
Hierarchical 131-2
historical data 89, 92, 143, 164
HYPE 42-3, 81, 110, 144, 159
HYPE service 80-1, 144, 159

I

identification 41, 51, 91, 111
Identifying customer 83
implementation 17, 30, 57, 72, 96, 98-9, 105, 142, 156
Implementing ITIL 156
Improvement Process 4, 156-7
improvements 45, 50, 67-8, 70, 85, 95, 109, 120, 124, 126, 143, 150-4, 156-7, 159-60
Technology improvements xf0b7 Process 159
Incident and Problem data 143
Incident and Problem Management 88, 129
Incident Management 4, 8, 18, 127, 130, 132, 134-5, 137, 145
management reports, Assist 139
Incident Management and Problem Management 130, 144
Incident Management process 134
incident process 133
incident resolution 133
incidents 19, 23, 44, 62, 65-9, 76-7, 88, 95-6, 102, 110, 130-6, 138, 144-5, 163
Incidents & Problems 23
incidents, security 75-7
industry 5, 9
information 13, 18, 23, 29-30, 38, 48, 56-61, 65, 75, 86-90, 92-3, 111, 140, 142-3, 145, 167-8 [7]
configuration 97
consistent 59
interface 90
operational 128
record 90
reference 58
Managing 86
information exchanges 75
Information Security 75, 77, 83, 129, 143
Information Security Management (ISM) 3, 75-8, 142
Information Security Management and Access Management 67
Information Security Management Considerations 80
Information Security Manager 78
Information Security Measure Matrix 78
Information Security Mgt 21
Information Technology Infrastructure Library 9
Informing users of available services 83
infrastructure 12, 14, 23, 39, 49, 63-4, 67, 71, 77, 85-6, 88-90, 92-3, 99, 116-17, 122, 145-6 [10]
infrastructure components 64, 72
Infrastructure Library 9
Initial Testing 72
initiatives 31-2, 35
input 15, 36, 56, 123, 128-9, 143
INPUTS SUB-PROCESS OUTPUTS 65
instant messaging 42
integrity 75, 92-3, 99, 142
interfaces 40-1, 47-8, 55, 59-60, 90, 129, 141-2
Internet Service Providers, see ISP
inventories 90

investments 29, 57, 62, 67, 158
ISM, see Information Security Management
ISO/IEC 4, 168
ISP (Internet Service Providers) 27-8, 81
IT Service Management, see ITSM
items 59-60, 105, 156
ITIL, official 5
ITIL framework 9
ITIL processes 49
ITIL V2 21
ITIL V3 21
ITILs 20
ITSM (IT Service Management) 3, 5-9, 12, 14, 19, 29, 65, 75, 88, 137, 149, 156-7, 161, 168
ITSM processes 67, 156
ITSM set of organizational capabilities 12

J

Japan 157
judgments 87

K

KEDB 88, 135, 163
Key Performance Indicators, see KPIs
Key Performance Indicators for Incident Management 134
Key Performance Indicators of Service Level Management 153
knowledge 5-6, 20, 23, 59-60, 67, 86-8, 111, 115, 131
Knowledge Management 4, 86, 111
Knowledge Management System 86
Knowledge Process Outsourcing 56
Known Error 19, 23, 88, 109, 135-7, 143-5, 163
Known Error Database 88, 135, 163
KPIs (Key Performance Indicators) 41, 79, 101, 121, 154-5, 158

L

layers 8
lessons 138
license 11, 16, 19, 26, 38, 55, 60, 72, 87, 93, 97, 100, 108, 150
lifecycle 19, 23, 30, 48, 56, 58, 88-9, 92-3, 126, 142, 158, 164
lifecycle phases 23, 41, 49, 58, 79, 109, 115, 143, 154, 158
line, Organization 134
location 82, 104
Logistics 104-5
logs 39, 80, 144

M

Maintainability 67, 163-4
maintenance 57-8, 60, 66, 146
Major Concepts of ITIL 21
management 5, 13, 17, 23, 29, 34, 48, 65, 67, 72, 74, 88, 115, 125, 132, 146-7 [2]
manages 56, 62-3, 88
market spaces 13, 32-3, 40
markets 33, 36
maturity, tactical process 155
meal 14, 59
Mean Time 83

Mean time between Failures, see MTBF
Mean time between System Incidents, see MTBSI
Mean Time to Restore Service 83, 164
Mean time to Restore Service, see MTRS
Measurement systems 48
mechanisms 59, 95-6, 141
menu 59, 141
metrics 48, 70, 101, 121, 150, 154, 158-9
model 40, 65, 108, 111, 115, 160
 logical 89-90, 93
momentum 150
money 8, 12, 15, 35, 55
monitor 33, 65, 68, 104, 146, 154, 156, 160
monitoring 64, 67, 128-9, 132, 160
MTBF (Mean time between Failures) 69-70, 83, 163
MTBF/MTBSI 69
MTBSI (Mean time between System Incidents) 69-70, 83, 163
MTRS (Mean time to Restore Service) 69-70, 83

N

natural process 19
new suppliers 57-8

O

objectives 3-4, 8, 25, 29, 37, 45, 47, 55, 59-60, 76, 85, 91, 107, 115, 149-50, 155-6 [1]
Objectives of Service Strategy 25
OBJECTIVES of SERVICE STRATEGY 3
OGC 11, 16, 19, 38, 55, 60, 72, 87, 93, 97, 100, 108, 150
OLAs (Operational Level Agreement) 23, 50-1, 70, 79, 83, 109, 152, 164
operation phase, Service 23
Operational Level Agreement, see OLAs
Operational Level Agreements 50-1, 164
 process reviews 83
operational management 13, 15, 34, 72-3
operational process manager, Significant Change 98
operations 85, 91, 95, 103, 106, 115, 122
 maintaining service 32
Operations Control 125, 147
Operations Management 4, 12, 122, 124-5, 144
organization 5-9, 12-16, 25, 28-9, 33-5, 37-41, 51-4, 56-7, 59, 61-2, 76-7, 86-7, 116-17, 119-20, 122, 124-6 [9]
 external 56-7
 international 49, 119
 large 33, 54
 mature 61
 outsourcing 56
 physical 119
 proactive 117
 retail 103
 service provider's 33
 smallest 122
 umbrella 13
Organization & Impl 72
organization display fuzzy process 32
organizational capabilities 5
 specialized 5, 12
organizational changes 17

organizational goals 8
organizational objectives 5, 40, 95
Organizational Procedural Technical Physical 78
organizational structure 118
 suggested 118
organization's focus 117
organization's objectives 8
organizations 7, 56, 62, 129
organization's assets 75
organization's business processes 122, 126
organization's capability 25
organization's day 124
organization's objectives 8
organization's release policy 102
organization's strategy 32
OS Business systems 91
outage 66
overspend 116-17
owner 13
ownership 12, 14, 18, 132, 164

P

packages 27
 developing service 28
Particularly Capacity and Availability Management 38
parties 26, 52, 59, 108, 141
pathways 4, 167-8
patterns 16, 36, 38, 40
Patterns of Business Activity, see PBA
Payroll Service 13
PBA (Patterns of Business Activity) 23, 37-8, 41
performance 15, 26-7, 39, 41, 50, 57, 63-5, 128, 143, 146, 154-5
person 12-13, 15, 92, 108
perspectives 3, 6, 34, 45, 75, 78, 83
phases 20, 23, 29, 42, 49-50, 65, 85, 103, 115, 149, 156
Physical databases 91-2
physical locations 75, 82, 119
PIR (Post Implementation Review) 109, 112
planning 68, 72, 74, 91, 104
plans 31, 50, 56, 68, 100, 143, 153, 156, 160
 business communication 159
 Service Operational 48
player 17, 118
Point of Sale Services 8
portfolio 30-3, 42
Post Implementation Review (PIR) 109, 112
practices, best 9, 19
prices 26, 51, 59
prioritization 131-2
Proactive Problem Management 137-8
Proactive Problem Management analyses Incident Records 137
proactive Service Management 117
Problem Management 4, 82, 88, 129-30, 133, 135-7, 139, 145
 activities of Reactive 137-8
 Incident Management 127
Problem Management and Change Management 145
Problem Mgt Service Asset 21
Problem Review 138

problems 19, 36, 39, 65, 67, 88, 102, 135-8, 145-6, 163
Process and Function organization improvements 158
process expertise 56
Process Improvements 23, 150, 158
process manager 13, 15
process manages 89
process metrics 109, 143, 154
Process metrics and KPIs 41, 79
process owner 13, 15, 164
Process Owners 154
Process Package 45
Process, Commitment 101
Process, Report provision 70
processes 5-6, 8, 12-13, 15-19, 21-3, 31-2, 36-7, 41-2, 44-5, 47-9, 95-7, 111-12, 134-6, 142-4, 149-54, 163-5 [18]
Processes & Functions 15
PROCESSES & FUNCTIONS 3
processes 150
 integrated centralized 7
processes, Analyses 152
products 5, 8, 45, 57, 152, 165
profiles 38, 63, 65
Project Management 100
Projected Service Outage (PSO) 96, 146
projects 13, 35, 112, 121
Proprietary knowledge of organizations 9
Protecting information 75
providers 26-7, 33, 52
 modern Service 26
PSO (Projected Service Outage) 96, 146

Q

quality 6, 14, 23, 41, 47, 56, 79, 86, 117, 119, 121, 130, 154, 156, 163, 168
 perceived 14

R

RACI 18
RACI Model 18
RCI 18
Reactive Problem Management 137
recover 73, 75, 77
recovery time 68-9
reduction 70, 130, 145, 163
redundancy 41
Release and Deployment Management 4, 102-3, 112
Release Packages 102, 109
Release Unit 102
releases 9, 23, 85, 88, 92, 101-5, 107-9, 111, 138, 146, 155, 164
reliability 41, 66-7, 69-70, 164
reports 13, 18, 39, 63, 65-6, 143, 146, 152, 154, 156, 160
Request for Change:, see RFCs
Request Fulfilment 140-1
 scope of 140
request models 140-1
requests 23, 89, 96, 119, 121, 140-1, 143, 145, 158, 164
requirements
 customer's 160
serviceability 80

Requirements Portfolio and Service Catalogue 44
resolution 131-2
resolution rate, first-time 119
resources 12, 15, 29, 31, 35, 39-40, 48, 62-3, 72, 85-6, 99, 105, 122, 141, 152, 163-4
 required 31, 35, 40
responsibilities 5, 7, 12, 15, 17-18, 51-2, 65, 70, 74, 78, 91, 99-100, 105-6, 113, 118, 126-7 [4]
Responsibilities Service Asset Management 93
Responsibilities Service Level Manager 152
responsiveness 116
restaurant 14, 59
restore 68-9, 130
restore point 68-9
Retired services 32
Retired Services 30
retiring 33
Return on Investment, see ROI
rewards 31, 33
RFCs (Request for Change:) 96-8, 100-1, 132, 145, 164
Risk Assessment 71-2
risks 12-14, 25, 29, 31, 33, 40, 85, 99, 103, 153, 164
 information security 76
ROI (Return on Investment) 33, 143, 158
Roles and Responsibilities 74, 100, 106, 122, 124, 126, 133
Roles and Responsibilities for Capacity Management 65
Roles and Responsibilities Service Asset Management 93
Roles and Responsibilities Service Level Manager 152
root cause 130, 135-6
root-cause 130, 133, 135-6
Row 18

S

Sale Services 8
SCD (Supplier and Contract Database) 55, 57-8, 164
schedule, service release 83
scope 9, 30, 59-60, 71, 90-1, 115, 140, 149, 156
 organization's 32
security 27, 42, 67, 75-6, 78, 80, 83
security process 78
self help 59, 120-1
self-help 140-1
senior management 74, 78, 101
Service Acceptance Criteria 79
Service Acceptance Criteria/Plan 108
Service Acceptance Test 108
service achievements 128
service agreements 146
Service and Process Improvements 23, 158
Service Asset & Configuration Management 82, 88, 111
Service Asset & Configuration Management work 106
Service Asset and Configuration Management 4, 40, 89, 94, 112
Service Asset and Configuration Management Considerations 110
service assets 36, 40, 79, 89, 93, 102, 164
 changed 23
 deploy 40
service assets interact 40
service availability 23, 66-7, 96, 115, 140
service base 84
Service-based SLAs 53
service calls 119

Service Capacity Management 63, 65
Service Catalogue 23, 30, 36, 40, 42, 51-2, 59-61, 79
 Business 81
 Manages 152
Service Catalogue and Configuration Management System 60
Service Catalogue and Service Portfolio 60
Service Catalogue information 60
Service Catalogue Management 3, 59
Service Catalogue Mgt 21
service changes 107
Service Component Build and Test 108
service components 79, 102, 104, 116
 updated 104
Service Continuity Management 3, 71-2, 82-3
Service Continuity Management, Information Security 49
Service Continuity Mgt 21
Service Delivery 6, 49, 51, 143, 146
Service Delivery and Support 118
service demand 36
service deployment 104
Service Derivation 44
Service Design 3, 21, 23, 40-1, 45, 47-50, 58, 79, 104, 107, 109-10, 124, 143, 149, 158, 162
Service Design and Service Transition Processes 105
Service Design and Transition 143
service design book 22
service design criteria 108
service design outputs 79
Service Design Packages 48, 79
Service Design Phase 58, 67, 149
service design processes 3, 49, 81
Service Design Review Questions 3, 82
Service Design Scenario 3, 80
Service Design Service Transition Service Operation 21
Service Design Summary 3, 79
service design volume 5
Service Desk 4, 12, 18, 51, 82, 96, 103, 105, 112, 119-21, 127, 132-4, 140-2, 144-6
 centralized 119
 in-services 110
Service Desk for Support 28
Service Desk Function 21
service desk hours 75
Service Desk Managers 121
Service Desk Structures 119
Service Desk Types 119
Service Desks, multiple 119
service disruption 73
service downtime 68
Service Economics 25
service elements 107
service HYPE 42
service impact 80
service improvement initiative 151
Service Improvement Plans 23, 152, 155, 159, 164
Service Improvement Programme (SIP) 112, 159, 164
service improvements 65, 158
 identifying potential 152
 Continual 9, 38, 41
Service Incidents 163
service information 81
service initiatives 31

service investments 31-3
Service Knowledge Management System, see SKMS
Service Knowledge Management System and Requirements Portfolio 44
Service Knowledge Management System and Service Catalogue 44
Service Level Achievement Baseline 155
service level achievements 152-3
Service Level Agreement, see SLAs
Service Level Agreement Structures 53
Service Level Agreements 44, 51-2, 59, 89, 130, 164
Service Level Agreements structures 84
Service Level Agreements, identification 152
Service Level Management
 efficient 153
 primary goal of 50, 151
 response actions 129
Service Level Management (SLM) 3-4, 8, 21-2, 39, 44, 49-51, 54, 68, 82-3, 112, 149, 151-2, 159, 164
Service Level Management and Financial Management 63
Service Level Management Considerations 80
Service Level Manager 154, 164
Service Level Mgt 21
Service Level Package Example 28
Service Level Packages 27-8, 42, 44-5, 80
Service Level Requirements, see SLR
Service Levels 42, 44, 53, 63, 84, 115, 143, 146, 150
 accurate estimations of 85, 109
Service Lifecycle 3, 14, 19-22, 25, 38, 40, 44-5, 58, 65, 86, 104, 107, 143, 149-50
service lifecycle approach 23
Service Lifecycle Model 19
Service Lifecycle Phases 21, 23
Service Management 5, 7, 9, 12, 20, 25, 44, 107, 161
service management activities 23
service management practices 7
Service Management processes 89, 129, 149, 154, 168
 inefficient 107
service management tools 141
Service Measurement 4, 154, 159
Service Measurement & Reporting 21
Service Measurement and Reporting 150
service metrics 154
Service Models 41, 108
Service Offerings 59
Service Operation 4, 17, 21, 23, 40-1, 43-4, 49, 58, 79, 81, 102, 109, 115-16, 118, 127, 143 [6]
 normal 130
Service Operation and Continual Service Improvement 45
Service Operation Functions 4, 118
Service Operation Phase 67
Service Operation Processes 4, 127, 143
Service Operation Review Questions 4, 145
Service Operation Scenario 4, 144
Service Operation Summary 4, 143
Service Operational Criteria/Plan 108
Service Operational Readiness Test 108
Service Operations activities 45
Service Operations key roles 115
Service Operations processes 143
Service Operation's key roles 116
service organization 5, 8, 31
Service Owners 13, 45, 154, 164
Service Package Example 27

Service Packages 26-8, 39, 42, 45, 108
 multiple 28

Service Packages and Service Level Packages 3, 27-8

service page 108

service performance 23, 63, 65

Service Portfolio and Catalogue 57

Service Portfolio information 23

Service Portfolio Management 3, 29, 31, 33, 59, 83
 Improved 34

Service Portfolio Management Considerations 42

Service Portfolio Mgt 21

Service Portfolios 25, 29-33, 40-1, 44, 47-8, 59, 79, 150
 multiple 30
 refreshed 158

Service Program, Service Transition Plan 48

service provider 13, 20, 26, 28, 30-1, 34, 36-7, 50-2, 54, 56, 59, 69, 88, 136, 150, 164 [1]

service provider restores 69

Service Provider's response 30

service provision 62, 66, 71, 89, 119, 153

service provision, learning 7

service quality 56, 80, 95, 117, 130
 losing 117

service quality, Rotation 121

Service Release Package Test 108

Service Release Test Criteria 108

service requests 23, 96, 120, 140-1, 146

Service Requirements 108

service retirement 31, 48, 105

Service Review Criteria/Plan 108

Service Reviews 65

Service Solutions 47-8, 108

Service Strategy 3, 21, 23, 25-6, 29, 37, 40-2, 44-5, 47, 64, 79, 109, 143, 150, 158, 162
 Developing 25

Service Strategy and Continual Service Improvement 45

Service Strategy outputs 41

Service Strategy processes 39

Service Strategy Processes 3, 29

Service Strategy Review Questions 3, 44

Service Strategy Service Scenario 3, 42

Service Strategy Summary 3, 40

service support 42

Service Support Package 45

Service Transition 3, 23, 40-1, 44-5, 79, 85, 109, 111, 143, 158, 162

Service Transition and Service Operation 45

Service Transition outputs 109

Service Transition Plans 79

Service Transition processes 107

Service Transition Processes 4, 86

Service Transition Review Questions 4, 111

Service Transition Scenario 4, 110

Service Transition Summary 4, 109

Service Utility 26-7

Service Utility and Service Warranty 27, 36

Service Validation 4, 107, 111-12

Service Validation & Testing 21, 106

Service Validation and Testing Considerations 110

Service Validation and Testing process 107

Service Validation Criteria 41

Service Valuation 36

Service Value 3, 26, 29-30

Service Warranty 26-7
Service, improved service alignments 79
service 70
Serviceability 67, 164
services
 based 57
 brand instant messenger 42
 broadband internet 27
 bundled 27
 business 29
 common 32, 140-1
 core 27
 cost-effective 79
 courier 71
 decommissioned 30
 deploy 105
 dining 59
 end-to-end 14, 154
 external supplier 81
 fix 117
 improved 124
 improving 151
 justifiable service quality 7
 likely disrupt 130
 live 30, 99
 modified 6, 51, 85, 102, 106-7
 modifying 40
 operational 59
 organization's 142
 provider's 30
 redundant 33, 42, 52
 shared 61, 115
 standard 140
 supporting 27, 38, 41, 60-1, 79
 transfer 105
 voice 71
 web 115
Service Level Requirements 48
Services and Service Packages 26
Services and Service Portfolios 40, 47
services/CIs 164
services investment 31
Services Staff 101
services 63
 requested standard 140
services, Developing 70
services, Plans 63
Service Transition 81
Service's attributes 27
Shared Service Providers 13
SIP (Service Improvement Programme) 112, 159, 164
skills 5, 14, 59, 65, 67, 70, 74, 78, 106, 110, 120-1, 126, 133, 139, 152
 technical 122, 146
SKMS (Service Knowledge Management System) 57, 88, 110, 135, 164
SLA structure 53
SLAs (Service Level Agreement) 23, 44, 50-4, 59, 65, 70-1, 79, 84, 89, 96, 109, 121, 130, 152, 158-9,
 164 [1]
SLAs, incident management team, Ensure 133
SLM, see Service Level Management

SLM process and Service Level Agreement 50
SLR (Service Level Requirements) 50-1, 65, 79, 112, 164
software 6, 28, 35, 71, 91, 95, 102, 104, 146
 back-end process-handling 120
sources 5, 9, 13, 30, 87, 90, 120, 140
SSIP (Supplier service improvement plans) 56, 164
stability 115-17, 124
staff 5-7, 11, 14, 38, 42, 59, 66-7, 74, 78, 86, 117, 121, 123-4, 130, 138, 146
staff members 7, 16, 71, 118, 120
stakeholders 5-7, 12, 15, 20, 44, 107
Standard Changes 96, 112, 140-1
standards 9, 12, 15, 40, 107, 168
Status Accounting 89, 91-2, 111, 164
status change, CI change/incident/problem history 92
status quo 115-16
Step Improvement Process 160
steps 4, 96, 149, 156-7, 160
Strategic business awareness 65
sub-processes collate 63
Sub-Processes of Problem Management 137
sub-services 63
Supplier and Contract Database, see SCD
Supplier Management 3, 51, 55-6, 58, 80, 83, 147
supplier management process activity 57
supplier processes 141
Supplier Service Improvement Plan 56, 164
Supplier service improvement plans (SSIP) 56, 164
supplier strategy 57
suppliers 55-8, 101, 136, 141
 external 5, 49-51, 67, 96, 108, 142, 164
Support considerations for Service Design 143
support services 19, 93, 115
support staff 105, 121, 123
Supporting Services Package 27-8, 45
symptoms 130
system boundaries 32
System Incidents 68, 83
systems
 information processing 75
 service management 48
 Computerized service desk 121

T

targets
 key service 52
 service level 50
Technical and Application Management functions 124, 142
technical infrastructure 122, 146
Technical Management (TM) 4, 12, 118, 122, 144, 146
Technical Management functions 123, 139
Technical Service Catalogue 60-1
techniques 37-8, 130, 163
technological environments 115-16
technology 5, 8, 26, 59-60, 65, 104, 115, 119-22, 141, 143, 146
technology architectures 48
technology components 121
termination 57-8
Terminology 12, 35, 51, 56, 67, 71, 73, 75, 89, 95, 102, 119, 135
terminology, common 3, 11

test 85, 97, 99-101, 106, 108, 110
theartofservice.com 167-8
threats, process analyses 82
TM, see Technical Management
tools 6, 12, 15, 18, 47-8, 78, 87-8, 92, 103, 115, 121, 141, 143, 163
training 17, 104-5, 138, 143-4
transactions 59
 Business 75
Transitioning New and Changed Services 106
tuning 64, 82, 143, 165
types 42, 49, 53, 56-7, 80, 84, 102, 122, 128, 140, 145, 154

U

UC (Underpinning Contract) 50-1, 55, 70, 165
UCs 23, 51, 79, 109
Underpinning Contract, see UC
user base 103
user/business 131
user calls 146
user/customer 141
users 15-16, 39, 49-50, 61, 64, 66, 69, 80, 82-4, 88, 96, 104-5, 116-17, 132-3, 140-2, 144-5 [7]
 authorized 67, 142
utility 26-8, 40, 42, 44-5, 71, 165

V

validation results 23, 109
value 5, 12, 14-15, 17, 26-7, 34-7, 40, 42-4, 55, 89, 102, 107, 143, 145, 154, 158 [2]
value creation 26
VBFs, see Vital Business Function
version 9, 19, 21, 37
video conferencing 42
Virtual Service Desk structure 82, 120
vision 150, 154, 160
Vital Business Function (VBFs) 67-8, 71-2, 165
VOI 158
VOIP 42

W

warranty 26-8, 38, 40-2, 44, 165
website 140-1, 167-8
weeds 130
whats 99
wisdom 86-7, 111
work, service lifecycle 3, 23
work orders 97-8
workarounds 132, 135, 138, 144, 163, 165